(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年11 月18 日 (18.11.2004)

PCT

(10) 国際公開番号
WO 2004/100154 A1

(51) 国際特許分類[7]: G11B 20/10, 20/12, 27/00, G06F 12/14, H04L 9/00, 9/32

(21) 国際出願番号: PCT/JP2004/006324

(22) 国際出願日: 2004 年4 月30 日 (30.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-125968 2003 年4 月30 日 (30.04.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 浅野 智之 (ASANO, Tomoyuki) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 佐藤 隆久 (SATOH, Takahisa); 〒1110052 東京都台東区柳橋２丁目４番２号 創進国際特許事務所 Tokyo (JP).

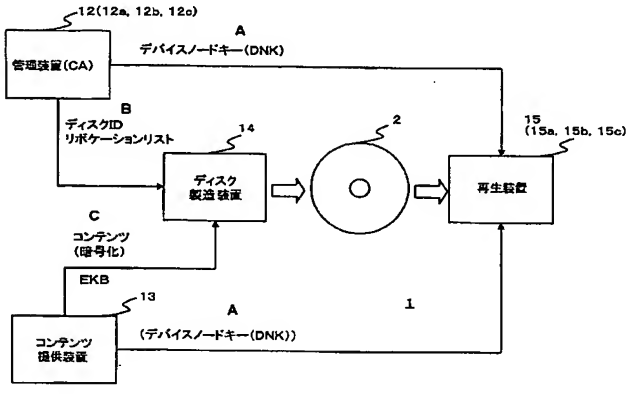
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: DATA PROCESSING METHOD, PROGRAM THEREOF, DEVICE THEREOF, AND RECORDING MEDIUM

(54) 発明の名称: データ処理方法、そのプログラム、その装置および記録媒体



12...MANAGEMENT DEVICE (CA)
A...DEVICE NODE KEY (DNK)
B...DISC ID REVOCATION LIST
C...CONTENT (ENCRYPTION)
13...CONTENT PROVIDING DEVICE
14...DISC MANUFACTURING DEVICE
15...REPRODUCTION DEVICE

(57) Abstract: A management device (12) generates a plurality of different signature data by using its secret key and provides them as disc ID to a disc manufacturing device (14). The disc manufacturing device (14) manufactures a plurality of disc-shaped recording media (2) where the aforementioned disc ID are recorded. A reproduction device (15) reads out a disc ID from a disc-shaped recording medium (2) and verifies it according to public key data on the management device (12) before performing reproduction.

(57) 要約: 管理装置１２は、自らの秘密鍵を用いて異なる複数の署名データを生成し、これをディスクＩＤとしてディスク製造装置１４に提供する。ディスク製造装置１４は、複数の上記ディスクＩＤをそれぞれ記録した複数のディスク型記録媒体２を製造する。再生装置１５は、再生装置１５を再生する前に、ディスク型記録媒体２からディスクＩＤを読み出し、これを管理装置１２の公開鍵データを基に検証する。

WO 2004/100154 A1

KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領 の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

データ処理方法、そのプログラム、その装置および記録媒体

技術分野

本発明は、記録媒体を識別する識別データに係わる処理を行うデータ処理方法、そのプログラム、その装置および記録媒体に関する。

背景技術

光ディスクなどの記録媒体を用いてコンテンツを提供する場合に、その記録媒体が不正に複製されると、コンテンツ提供者の利益が不当に害される。

このような問題を解決するために、個々の記録媒体を識別するＩＤを各記録媒体に記録し、そのＩＤを基に不正に複製された記録媒体を特定するシステムが知られている。

しかしながら、上述した従来のシステムでは、記録媒体に記録されたＩＤが改竄されたものであるか、並びに正当な権限を有する者が生成したかを検証ことができないという問題がある。

発明の開示

本発明は上述した従来技術の問題点に鑑みてなされ、識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法、そのプログラムおよびその装置を提供することを第１の目的とする。

また、本発明は、上記第１の目的を達成するデータ処理方法、そのプログラム、その装置によって生成された識別データを適切に検証できるデータ処理方法、そのプログラムおよびその装置を提供することを第２の目的とする。

また、本発明は、上述した第１の目的を達成するデータ処理方法、そのプログラム、その装置によって生成された識別データを記録した記録媒体を提供することを第３の目的とする。

上述した目的を達成するために、第１の発明のデータ処理方法は、記録媒体を識別する識別データを生成するデータ処理方法であって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第１の工程と、前記第１の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第２の工程とを有する。

第１の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する。

次に、第２の工程において、前記第１の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる。

上記各工程はデータ処理装置が実行する。

第２の発明のプログラムは、記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第１の手順と、前記第１の手順で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第２の手順とを有する。

第３の発明のデータ処理装置は、記録媒体を識別する識別データを生成するデータ処理装置であって、前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第１の手段と、前記第１の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第２の手段とを有する。

第３の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、前記識別データの管理元の秘密鍵データを用いて、複数

の異なる署名データを生成する。

次に、第２の手段が、前記第１の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる。

第４の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する工程を有する。

当該工程はデータ処理装置によって実行される。

第５の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手順を有する。

第６の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手段を有する。

第７の発明のデータ処理方法は、記録媒体を識別する識別データを生成するデータ処理方法であって、前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する第１の工程と、前記第１の工程で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第２の工程とを有する。

第７の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数

の異なる署名データを生成する。

次に、第２の工程において、前記第１の工程で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる。

第８の発明のプログラムは、記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する第１の手順と、前記第１の手順で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第２の手順とを有する。

第９の発明のデータ処理装置は、記録媒体を識別する識別データを生成するデータ処理装置であって、前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する第１の手段と、前記第１の手段で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第２の手段とを有する。

第９の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する。

次に、第２の手段が、前記第１の手段で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる。

第１０の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識

別する識別データの正当性を検証するデータ処理方法であって、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する第１の工程と、前記第１の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する第２の工程とを有する。

第１０の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する。

次に、第２の工程において、前記第１の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する。

上記各工程はデータ処理装置によって実行される。

第１１の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する第１の手順と、前記第１の手順で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する第２の手順とを有する。

第１２の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデー

タを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する第１の手段と、前記第１の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する第２の手段とを有する。

第１２の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成する。

次に、前記第１の手段が、前記第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する。

次に、第２の手段が、前記第１の手段で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する。

第１３の発明のデータ処理方法は、公開されたデータＭを２つの素数の積とし、ＴをＷ（Ｗ≧２）個の異なる素数ｐ（ｗ）の積とし、ｗを１≦ｗ≦Ｗの整数とし、Ｋを巡回群Ｚ＊Ｍの生成元とした場合に、Ｗ個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理方法であって、（ＫＴ／ｐ（ｗ）ｍｏｄＭ）を算出する第１の工程と、ｐ（ｗ）と前記第１の工程で算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の工程とを有する。

第１３の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する。

次に、第２の工程において、ｐ（ｗ）と前記第１の工程で算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる。

上記各工程は、データ処理装置によって実行される。

第１４の発明のプログラムは、公開されたデータＭを２つの素数の積とし、Ｔ

を W（W≧２）個の異なる素数ｐ（ｗ）の積とし、ｗを１≦ｗ≦W の整数とし、Ｋを巡回群Ｚ＊Ｍの生成元とした場合に、W 個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置が実行するプログラムであって、（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する第１の手順と、ｐ（ｗ）と前記第１の手順で算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の手順とを有する。

第１５の発明のデータ処理装置は、公開されたデータＭを２つの素数の積とし、ＴをＷ（Ｗ≧２）個の異なる素数ｐ（ｗ）の積とし、ｗを１≦ｗ≦Ｗの整数とし、Ｋを巡回群Ｚ＊Ｍの生成元とした場合に、Ｗ 個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置であって、（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する第１の手段と、ｐ（ｗ）と前記第１の手段が算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の手段とを有する。

第１５の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する。

次に、第２の手段が、ｐ（ｗ）と前記第１の手段が算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる。

第１６の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、前記識別データに含まれるデータｐが素数であるか否かを検証する第１の工程と、前記第１の工程で前記データｐが素数であると検証された場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて　（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する第２の工程と、前記第２の工程で算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第３の工程とを有する。

第１６の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、前記識別データに含まれるデータｐが素数であるか否かを検証する。

次に、第２の工程において、前記第１の工程で前記データｐが素数であると検証された場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて　（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する。

次に、第３の工程において、前記第２の工程で算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する。

上記各工程は、データ処理装置によって実行される。

第１７の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データに含まれるデータｐが素数であるか否かを検証する第１の手順と、前記第１の手順で前記データｐが素数であると検証された場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する第２の手順と、前記第２の手順で算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第３の手順とを有する。

第１８の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データに含まれるデータｐが素数であるか否かを検証する第１の手段と、前記第１の手段が前記データｐが素数であると検証した場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する第２の手段と、前記第２の手段が算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第３の手段とを有する。

第１８の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、前記識別データに含まれるデータｐが素数であるか否かを検証する。

次に、第２の手段が、前記第１の手段が前記データｐが素数であると検証した場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する。

次に、第３の手段が、前記第２の手段が算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する。

第１９の発明のデータ処理方法は、素数ｑ１とｑ２の積であり公開されたデータをＭとし、ｗを１≦ｗ≦Ｗの整数とし、Ｗ（Ｗ≧２）個の異なるデータをｅ（ｗ）とし、ｅ（ｗ）を巡回群Ｚ＊Ｍの生成元とし、e(w)とλ（Ｍ）は互い素であり、λ（Ｍ）を（ｑ１－１）と（ｑ２－１）との最小公倍数とした場合に、Ｗ個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理方法であって、巡回群Ｚ＊Ｍの生成元であるデータＳと、λ（Ｍ）を法としたときのｅ（ｗ）の逆数であるデータｄ（ｗ）と、上記データＭとを用いて、（Ｓｄ（ｗ）ｍｏｄＭ）を算出する第１の工程と、前記ｅ（ｗ）と前記第１の工程で算出した（Ｓｄ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の工程とを有する。

第１９の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、巡回群Ｚ＊Ｍの生成元であるデータＳと、λ（Ｍ）を法としたときのｅ（ｗ）の逆数であるデータｄ（ｗ）と、上記データＭとを用いて、（Ｓｄ（ｗ）　ｍｏｄＭ）を算出する。

次に、第２の工程において、前記ｅ（ｗ）と前記第１の工程で算出した（Ｓｄ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる。

上記各工程は、データ処理装置によって実行される。

第２０の発明のプログラムは、素数ｑ１とｑ２の積であり公開されたデータを

Mとし、wを１≦ｗ≦Wの整数とし、W（W≧２）個の異なるデータをｅ（ｗ）とし、ｅ（ｗ）を巡回群Ｚ＊Mの生成元とし、e(w)とλ（M）は互い素であり、λ（M）を（ｑ１－１）と（ｑ２－１）との最小公倍数とした場合に、W 個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置が実行するプログラムであって、巡回群Ｚ＊Mの生成元であるデータＳと、λ（M）を法としたときのｅ（ｗ）の逆数であるデータｄ（ｗ）と、上記データＭとを用いて、（Ｓｄ（ｗ）　ｍｏｄM）を算出する第１の手順と、前記ｅ（ｗ）と前記第１の手順で算出した（Ｓｄ（ｗ）　ｍｏｄM）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の手順とを有する。

第２１の発明のデータ処理装置は、素数ｑ１とｑ２の積であり公開されたデータをＭとし、ｗを１≦ｗ≦Wの整数とし、W（W≧２）個の異なるデータをｅ（ｗ）とし、ｅ（ｗ）を巡回群Ｚ＊Mの生成元とし、e(w)とλ（M）は互い素であり、λ（M）を（ｑ１－１）と（ｑ２－１）との最小公倍数とした場合に、W個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置であって、巡回群Ｚ＊Mの生成元であるデータＳと、λ（M）を法としたときのｅ（ｗ）の逆数であるデータｄ（ｗ）と、上記データＭとを用いて、（Ｓｄ（ｗ）　ｍｏｄM）を算出する第１の手段と、前記ｅ（ｗ）と前記第１の手段が算出した（Ｓｄ（ｗ）　ｍｏｄM）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の手段とを有する。

第２１の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、巡回群Ｚ＊Mの生成元であるデータＳと、λ（M）を法としたときのｅ（ｗ）の逆数であるデータｄ（ｗ）と、上記データＭとを用いて、（Ｓｄ（ｗ）　ｍｏｄM）を算出する。

次に、第２の手段が、前記ｅ（ｗ）と前記第１の手段が算出した（Ｓｄ（ｗ）　ｍｏｄM）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる。

第２２の発明のデータ処理方法は、記録媒体に割当てられた当該記録媒体を識

別する識別データの正当性を検証するデータ処理方法であって、前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ ｍｏｄＭ）を算出する第１の工程と、前記第１の工程で算出した（Ｉｅ ｍｏｄＭ）を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第２の工程とを有する。

第２２の発明のデータ処理方法の作用は以下のようになる。

先ず、第１の工程において、前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ ｍｏｄＭ）を算出する。

次に、第２の工程において、前記第１の工程で算出した（Ｉｅ ｍｏｄＭ）を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する。

第２３の発明のプログラムは、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ ｍｏｄＭ）を算出する第１の手順と、前記第１の手順で算出した（Ｉｅ ｍｏｄＭ）を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第２の手順とを有する。

第２４の発明のデータ処理装置は、記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ ｍｏｄＭ）を算出する第１の手段と、前記第１の手が算出した（Ｉｅ ｍｏｄＭ）を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第２の手段とを有する。

第２４の発明のデータ処理装置の作用は以下のようになる。

先ず、第１の手段が、前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ ｍｏｄＭ）を算出する。

次に、第２の手段が、前記第１の手が算出した（Ｉｅ ｍｏｄＭ）を復号鍵と

して用いて、前記記録媒体に記録された暗号データを復号する。

第２５の発明の記録媒体は、データを記録する記録媒体であって、前記記録媒体の管理元の秘密鍵データを用いて生成され、前記管理元の公開鍵データを基に正当性が検証され、当該記録媒体を識別する識別データを記録している。

第２６の発明の記録媒体は、データを記録する記録媒体であって、前記記録媒体の管理元の公開鍵データを用いて第１のデータを生成するために用いられる署名データと、前記第１のデータと比較して識別データの正当性を検証するために用いられる第２のデータとを含み前記記録媒体を識別する前記識別データを記録している。

第２７の発明の記録媒体は、暗号データを記録する記録媒体であって、素数であるデータｐと、前記暗号データを復号するために用いられるコンテンツ鍵データである（ＩＤＫｅｙｐ　ｍｏｄＭ）を前記データｐと公開されているデータＭと共に算出するために用いられるデータＩＤＫｅｙとを含み前記記録媒体を識別する識別データを記録している。

第２８の発明の記録媒体は、暗号データを記録する記録媒体であって、前記暗号データを復号するために用いられるコンテンツ鍵データである（Ｉｅ　ｍｏｄＭ）を、公開されているデータＭと共に算出するために用いられるデータｅおよびデータＩとを含み前記記録媒体を識別する識別データを記録している。

図面の簡単な説明

図１は、本発明の実施形態に係わるディスク型記録媒体に記録されるデータを説明するための図である。

図２は、本発明の実施形態に係わるコンテンツ提供システムの全体構成図である。

図３は、図２に示す管理装置の構成図である。

図４は、図３に示す管理装置によるディスクＩＤの生成処理を説明するための

フローチャートである。

図５は、図２に示すディスク製造装置の構成図である。

図６は、図５に示すディスク製造装置によるディスク製造手順を説明するためのフローチャートである。

図７は、図１に示すディスク型記録媒体に記録されるリボケーションリストＤＩＲＬのデータ構成を説明する図である。

図８は、ＭＡＣ値生成処理例を示す図である。

図９は、各種キー、データの暗号化処理、配布処理について説明するツリー構成図である。

図１０は、各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

図１１は、コンテンツ鍵の有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

図１２は、有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

図１３は、有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

図１４は、ツリー構成におけるカテゴリ分割を説明する図である。

図１５は、ツリー構成におけるカテゴリ分割を説明する図である。

図１６は、図２に示す再生装置の構成図である。

図１７は、図１６に示す再生装置の再生処理を説明するためのフローチャートである。

図１８は、図１７に示すステップＳＴ３２のディスクＩＤの検証処理を説明するためのフローチャートである。

図１９は、図１７に示すステップＳＴ３８の再生処理を説明するためのフローチャートである。

図２０は、本発明の第２実施形態における管理装置のディスクＩＤの生成処理を説明するためのフローチャートである。

図２１は、本発明の第２実施形態における再生装置による図１７に示すステップＳＴ３２のディスクＩＤの検証処理を説明するためのフローチャートである。

図２２は、本発明の第２実施形態における再生装置による図１７に示すステップＳＴ３８の再生処理を説明するためのフローチャートである。

図２３は、本発明の第３実施形態における管理装置のディスクＩＤの生成処理を説明するためのフローチャートである。

図２４は、本発明の第３実施形態における再生装置による図１７に示すステップＳＴ３２のディスクＩＤの検証処理を説明するためのフローチャートである。

図２５は、本発明の第３実施形態における再生装置による図１７に示すステップＳＴ３８の再生処理を説明するためのフローチャートである。

図２６は、本発明の第４実施形態における管理装置のディスクＩＤの生成処理を説明するためのフローチャートである。

図２７は、本発明の第４実施形態における再生装置による再生処理を説明するためのフローチャートである。

発明を実施するための最良の形態

これより図面を参照して本発明の好適実施例について説明していく。

＜第１実施形態＞

当該実施形態は、第１～第６および第２５の発明に対応した実施形態である。

〔ディスク型記録媒体２〕

図１は、本発明の実施形態に係わるディスク型記録媒体２（第２５の発明の記録媒体）に記録されるデータを説明するための図である。

ディスク型記録媒体２は、ＣＤ(Compact Disc)、ＤＶＤ(Digital Versatile Disk)、ＭＤ(Mini Disk)やその他のディスク型の記録媒体である。

ディスク型記録媒体２が第２５の発明の記録媒体に対応している。なお、本発明の記録媒体は、ディスク型以外に、フラッシュメモリなどの半導体記録装置や

その他の記録媒体であってもよい。

図１に示すように、ディスク型記録媒体２には、ディスクＩＤと、暗号化コンテンツデータＥＣＯＮＴと、暗号鍵情報ＥＫＢと、ディスクＩＤのリボケーションリストＤＩＲＬとが記録される。

ディスクＩＤは、ディスク型記録媒体２を識別するための識別データであり、消去や書き換えが困難であるようにディスク型記録媒体２に格納される。

ディスクＩＤが本発明の識別データに対応している。ディスクＩＤの生成方法については後述する。

なお、以下に説明する実施形態では、ディスク状の媒体をコンテンツ格納情報記録媒体の例として示しているので、その識別データをディスクＩＤとして説明する。

フラッシュメモリ等の各種の情報記録媒体を利用した場合にもディスクＩＤに対応する識別データが設定される。

暗号化コンテンツデータＥＣＯＮＴは、暗号化されたコンテンツデータであり、暗号化コンテンツデータＥＣＯＮＴを復号するためのコンテンツ鍵データは、例えば階層型鍵データ配信構成によって、正当なコンテンツ利用機器としての再生装置に提供されるデバイスノード鍵データ（ＤＮＫ：Device Node Key）に基づいて、ディスク型記録媒体２に格納された暗号鍵情報である有効化鍵ブロック（ＥＫＢ：Enabling Key Block）の復号処理等によって取得される。

階層型鍵データ配信構成によるデバイスノード鍵データＤＮＫの提供、およびデバイスノード鍵データＤＮＫに基づく有効化鍵ブロックＥＫＢの復号処理による鍵取得処理の詳細については後述する。

また、ディスクＩＤのリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）は、不正コピー等が行われたと認定されたディスク、例えば市場に不正なコピーコンテンツを格納したＣＤ－Ｒが発見された場合に、その不正ＣＤ－ＲにコンテンツとともにコピーされたディスクＩＤを抽出し、リスト化したデータで

ある。リボケーションリストＤＩＲＬの生成、管理、ディスク製造者に対するリスト情報提供は、特定の信頼される管理局（ＣＡ：Central Authority）が実行する。

〔システム構成〕

図２は、本発明の第１実施形態に係わるコンテンツ提供システム１の構成図である。

図２に示すように、コンテンツ提供システム１は、管理局ＣＡが使用する管理装置１２と、コンテンツプロバイダが使用するコンテンツ提供装置１３と、ディスク製造者が使用するディスク製造装置１４と、ユーザが使用する再生装置１５とを有する。

ここで、管理装置１２が第２および第３の発明のデータ処理装置に対応している。

また、再生装置１５が第５および第６の発明のデータ処理装置に対応している。

なお、本実施形態では、再生装置１５を例示するが、ディスク型記録媒体２に記録されたディスクＩＤの正当性を検証し、その結果を基に処理を行うものであれば、再生装置１５の他に、例えば、ディスク型記録媒体２から読み出したコンテンツデータを記録または編集などを行うデータ処理装置を用いてもよい。

管理装置１２が、前述したディスクＩＤとリボケーションリストＤＩＲＬとを生成してディスク製造装置１４に提供する。

また、コンテンツ提供装置１３が、暗号化コンテンツＥＣＯＮＴと有効化鍵ブロックＥＫＢとをディスク製造装置１４に提供する。

ディスク製造装置１４は、管理装置１２から受けたディスクＩＤおよびリボケーションリストＤＩＲＬと、コンテンツ提供装置１３から受けた暗号化コンテンツデータＥＣＯＮＴと有効化鍵ブロックＥＫＢとを記録したディスク型記録媒体２を製造する。

ユーザは、ディスク型記録媒体２を例えば購入し、再生装置１５にセットする。

再生装置１５は、ディスク型記録媒体２に記録されたディスクＩＤが正当であると検証し、当該ディスクＩＤがリボケーションリストＤＩＲＬ内に存在しないことを確認し、自らのデバイスノード鍵データＤＮＫに基づいて有効化鍵ブロックＥＫＢから適切なコンテンツ鍵データを取得したことを条件に、暗号化コンテンツデータＥＣＯＮＴを復号し、続いて再生する。

以下、図２に示すコンテンツ提供システム１を構成する各装置について詳細に説明する。

〔管理装置１２〕

図３は、図２に示す管理装置１２の構成図である。

図３に示すように、管理装置１２は、例えば、メインメモリ２２、セキュアメモリ２３、入出力インタフェース（Ｉ／Ｆ）２４、記録媒体インタフェース（Ｉ／Ｆ）２５、演算ユニット２６およびコントローラ２７を有し、これらがバス２１を介して接続されている。

メインメモリ２２は、演算ユニット２６およびコントローラ２７の処理に用いられる種々のデータのうち、セキュリティレベルが低いデータを記憶する。

セキュアメモリ２３は、演算ユニット２６およびコントローラ２７の処理に用いられる種々のデータのうち、セキュリティレベルが高いデータを記憶する。

セキュアメモリ２３は、例えば、ディスクＩＤの生成に用いられる管理局ＣＡの秘密鍵データなどを記憶する。

入出力インタフェース２４は、例えば、図示しない操作手段あるいはネットワークなどに接続され、管理装置１２が使用する種々のデータを入力する。

記録媒体インタフェース２５は、コントローラ２７の制御の基に生成されたディスクＩＤおよびリボケーションリストＤＩＲＬを記録媒体２９ａに書き込む。記録媒体２９ａは、コンテンツ提供装置１３に提供される。

また、記録媒体インタフェース２５は、コントローラ２７の制御の基に生成されたデバイスノード鍵データＤＮＫを記録媒体２９ｂに書き込む。

記録媒体２９ｂは、再生装置１５、あるいは再生装置１５の製造元に提供される。

演算ユニット２６は、コントローラ２７からの制御に基づいて、署名データを生成し、これを基にディスクＩＤを生成する。

また、演算ユニット２６は、リボケーションリストＤＩＲＬを生成する。

コントローラ２７は、プログラムＰＲＧ１（第２の発明のプログラム）を実行して管理装置１２の処理を統括的に制御する。

本実施形態における管理装置１２の機能（処理）は、コントローラ２７によるプログラムＰＲＧ１の実行に応じて規定される。

管理装置１２の機能（処理）の全部あるいは一部は、プログラムＰＲＧ１によって規定されてもよいし、ハードウェアによって実現されてもよい。

以下、図３に示す管理装置１２によるディスクＩＤの生成動作を説明する。

図４は、図３に示す管理装置１２によるディスクＩＤの生成動作を説明するためのフローチャートである。

図４において、ステップＳＴ２が第１の発明の第１の工程に対応し、ステップＳＴ３が第１の発明の第２の工程に対応している。

また、コントローラ２７がステップＳＴ２を実行することで第３の発明の第１の手段が実現され、ステップＳＴ３を実行することで第３の発明の第２の手段が実現される。

ステップＳＴ１：

管理装置１２のコントローラ２７は、デジタル署名のための鍵データである管理局ＣＡの公開鍵データ（第１の発明の公開鍵データ）および秘密鍵データ（第１～第３の発明の秘密鍵データ）、並びに署名生成および検証のためのパラメータを決定する。

コントローラ２７は、上記公開鍵データおよび上記パラメータを公開する。

コントローラ２７は、例えば、出力インタフェース２４からネットワーク上に

上記公開鍵データおよび上記パラメータを送信して上記公開を行う。

ステップＳＴ１の処理は、管理装置１２のセットアップ時に一度だけ行えばよい。

ステップＳＴ２：

管理装置１２は、入出力インタフェース２４を介して、コンテンツプロバイダから、コンテンツ（たとえば映画）のタイトルと，製造するディスク型記録媒体２の枚数Ｗ（Ｗ≧２）を入力し、これをメインメモリ２２に格納する。

演算ユニット２６は、任意のメッセージＭ（第１の発明の第２のデータ）と、乱数ｒ（ｗ）と、管理局ＣＡの秘密鍵データとを用いて、Ｗ個のデジタルの異なる署名データＳＩＧ（ｗ）（第１～第３の発明の署名データ）を生成する。

当該署名データＳＩＧ（ｗ）は、管理局ＣＡの上記秘密鍵データに対応する公開鍵データを用いて、その改竄の有無、並びに正当性を確認可能な形態で生成される。

ここで、ｗ＝１，２・・・，Ｗであり，ｒ（ｗ）はそれぞれ個別の乱数である。

なお、演算ユニット２６は、それぞれ個別のＷ個のメッセージＭ（ｗ）（必ずしも個別の乱数でなくてもよい）を基に、署名データＳＩＧ（ｗ）を生成してもよい。

演算ユニット２６は、上記署名データＳＩＧ（ｗ）の生成方法として、署名生成時に署名者が任意の乱数を使うことができる方法である、ＦＩＰＳＰＵＢ　１８６－２で米国標準の署名方式となっているＤＳＡや，その楕円曲線暗号版であるＥＣＤＳＡなどを用いている。ＤＳＡ(Digital Signature Alogorithm)はたとえば，岡本龍明，山本博資著，「現代暗号」，産業図書，１９９７のｐｐ．１７９－１８０に解説が記されており，ＥＣＤＳＡに関してｈｔｔｐ：／／ｇｒｏｕｐｅｒ．ｉｅｅｅ．ｏｒｇ／ｇｒｏｕｐｓ／１３６３／ｔｒａｄＰＫ／ｉｎｄｅｘ．ｈｔｍｌから入手可能な仕様書にその詳細が記されている。

ステップＳＴ３：

コントローラ２７は、ステップＳＴ１で決定したメッセージMあるいはM（w）とステップＳＴ２で生成した署名データＳＩＧ（w）とを用いて、（M，ＳＩＧ（w））の組もしくは（M（w），ＳＩＧ（w））の組をw番目のディスクＩＤ（w）として生成し、それをタイトルとともにディスク製造者にセキュアな状態で提供する。

具体的には、例えば、図３に示す記録媒体２９ａにディスクＩＤ（w）を記録してディスク製造者に提供する。

また、管理装置１２は、リボークする情報記録媒体のディスクＩＤを示すリボケーションリストＤＩＲＬを生成し、これもディスク製造者に提供する。

〔ディスク製造装置１４〕

図５は、図１に示すディスク製造装置１４の構成図である。

図５に示すように、ディスク製造装置１４は、例えば、入出力インタフェース３２、暗号処理部３３、メモリ３４、コントローラ３５および記録媒体インタフェース３６を有し、これらがバス３１を介して接続されている。

入出力インタフェース３２は、外部から供給されるデジタル信号を受信し、バス３１上に出力する。

入出力インタフェース３２は、例えば、コンテンツ提供装置１３からの暗号化コンテンツデータＥＣＯＮＴおよび有効化鍵ブロックＥＫＢを入力する。

また、入出力インタフェース３２は、上記記録媒体１９ａなどを介して管理装置１２からディスクＩＤ（w）およびリボケーションリストＤＩＲＬなどのデータを入力する。

なお、入出力インタフェース３２は、製造するディスクの数に応じた数のディスクＩＤ（w）を管理装置１２から受ける。

また、入出力インタフェース３２は、コンテンツ提供装置１３から記録媒体などを介して暗号化コンテンツデータＥＣＯＮＴおよび有効化鍵ブロックＥＫＢを入力する。

暗号処理部３３は、例えば、１チップのＬＳＩ(Large Scale Integrated Curcuit)で構成され、バス３１を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス３１上に出力する構成を持つ。

なお、暗号処理部３３は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

メモリ３４は、コンテンツ提供装置１３から受領した暗号化コンテンツデータＥＣＯＮＴおよび有効化鍵ブロックＥＫＢと、管理装置１２から受けたディスクＩＤおよびリボケーションリストＤＩＲＬとを格納する。

コントローラ３５は、ディスク製造装置１４の処理を統括的に制御する。

記録媒体インタフェース３６は、コントローラ３５の制御の基に、種々のデータを書き込んだ図１に示すディスク型記録媒体２を製造する。

以下、図５に示すディスク製造装置１４の動作例を説明する。

図６は、図５に示すディスク製造装置１４の動作例を説明するためのフローチャートである。

ステップＳＴ１１：

ディスク製造装置１４は、入出力インタフェース３２を介して、上記記録媒体１９ａを介してW個のディスクＩＤ（w）およびリボケーションリストＤＩＲＬを管理装置１２から入力してメモリ３４に書き込む。

ステップＳＴ１２：

ディスク製造装置１４は、入出力インタフェース３２を介して、有効化鍵ブロックＥＫＢをコンテンツ提供装置１３から入力してメモリ３４に書き込む。

ステップＳＴ１３：

ディスク製造装置１４は、入出力インタフェース３２を介して、暗号化コンテンツデータＥＣＯＮＴをコンテンツ提供装置１３から入力してメモリ３４に書き込む。

ステップＳＴ１４：

ディスク製造装置１４のコントローラ３５は、リボケーションリストＤＩＲＬ、有効化鍵ブロックＥＫＢおよび暗号化コンテンツデータＥＣＯＮＴをメモリ３４から読み出し、これらのデータを情報記録媒体（ディスク）に書き込んでマスターディスクを製造する。

ステップＳＴ１５：

コントローラ３５は、ステップＳＴ１４で製造したマスターディスクに基づくスタンパによるスタンプ処理により、複製としてのディスクを製造する。

ステップＳＴ１６：

コントローラ３５は、ステップＳＴ１５で製造したディスクに、メモリ３４から読み出したディスクＩＤ(w)を書き込んでディスク型記録媒体２を製造する。

ステップＳＴ１７：

コントローラ３５は、W枚のディスク型記録媒体２を製造したか否かを判断し、製造したと判断した場合には処理を終了し、そうでない場合にはステップＳＴ１５の処理に戻る。

このように、ディスク製造装置１４は、管理装置１２から受けたディスク型記録媒体２の数Wに応じて、それぞれの製造ディスクに異なるディスクＩＤ（w）を書き込む。

従って、市場に流通するディスク型記録媒体２にはそれぞれ異なるディスクＩＤ（w）が設定されていることになり、同一のディスクＩＤ（w）が記録された複数のディスク型記録媒体２が発見された場合は、不正なコピーが実行されているものと判断し、管理局ＣＡがリボケーションリストＤＩＲＬにそのディスクＩＤ（w）を書き込む更新処理を実行し、更新されたリストがディスク製造業者に提供され、新規ディスクには、そのリストが格納される。

ディスク型記録媒体２を購入したユーザが、再生装置１５にディスク型記録媒体２をセットし、コンテンツ再生処理を実行する際には、再生装置１５内のメモリに格納されたリボケーションリストＤＩＲＬとのバージョン比較が実行され、

更新されたリストがメモリに格納される。従って、ユーザの再生装置１５のメモリに格納されるリストは、随時更新される。

以下、管理装置１２が製造するリボケーションリストＤＩＲＬについて説明する。

図７は、図１に示すリボケーションリストＤＩＲＬを説明するための図である。

図７に示すように、リボケーションリストＤＩＲＬは、当該リボケーションリストＤＩＲＬが作成された時期に応じて値が増加するバージョン番号５１と、無効に（リボーク）すべきディスク型記録媒体２のディスクＩＤ（ｗ）を羅列したリボークディスクＩＤリスト５２と、バージョン番号５１とリボークディスクＩＤリスト５２に対する改竄検証値５３としての認証子が含まれる。

改竄検証値５３は、対象となるデータ、この場合はバージョン番号５１とリボークディスクＩＤリスト５２が改竄されているか否かを判別するために適用するデータであり、公開鍵暗号技術を用いたデジタル署名や、共通鍵暗号技術を用いたメッセージ認証コード（ＭＡＣ：Message Authentication Code）が適用される。

改竄検証値５３として公開鍵暗号技術を用いたデジタル署名を用いる際には、信頼できる機関、例えば上述の管理局ＣＡの署名検証鍵（公開鍵）を再生機が取得し、管理局ＣＡの署名生成鍵（秘密鍵）を用いて作られた署名を各再生機が取得した署名検証鍵（公開鍵）によって検証することで、バージョン番号５１とリボークディスクＩＤリスト５２が改竄されているか否かを判別する。

図８は、改竄検証値５３としてメッセージ認証コードＭＡＣを用いた際のＭＡＣ生成、検証処理を説明するための図である。

メッセージ認証コードＭＡＣは、データの改竄検証用のデータとして生成されるものであり、ＭＡＣ生成処理、検証処理態様には様々な態様が可能であるが、１例としてＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図８を基に説明する。

図８に示すように、対象となるメッセージ、この場合は、図７に示すバージョン番号５１とリボークディスクＩＤリスト５２を８バイト単位に分割し、（以下、

分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする)、まず、初期値（Initial Value（ＩＶ））とＭ１を排他的論理和する（その結果をＩ１とする)。

次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする)。

続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号ＭＡＣとなる。

ＭＡＣ値は、その生成元データが変更されると、異なる値となり、検証対象のデータ（メッセージ）に基づいて生成したＭＡＣと、記録されているＭＡＣとの比較を行い、一致していれば、検証対象のデータ（メッセージ）は変更、改竄がなされていないことが証明される。

ＭＡＣ生成における鍵Ｋ１としては、たとえば、階層型鍵データ配信構成によるデバイスノード鍵データＤＮＫに基づく有効化鍵ブロック（ＥＫＢ）の復号処理によって得られる鍵（ルート鍵データ）を適用することが可能である。また、初期値ＩＶとしては、予め定めた値を用いることが可能である。

〔階層型鍵配信ツリー構成〕

以下、ブロードキャストエンクリプション（Broadcast Encryption）方式の一態様である階層型鍵配信ツリー構成に従った鍵提供処理、再生機としての再生装置管理構成について説明する。

図９の最下段に示すナンバ０～１５がコンテンツ利用を行なうユーザデバイスである。本実施形態では、当該ユーザデバイスは、図２に示す再生装置１５に対応している。

図４に示す階層ツリー（木）構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図

９に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノード鍵データ）および各リーフのリーフ鍵データからなる鍵データセット（デバイスノード鍵データＤＮＫをメモリに格納する。

図９の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフ鍵データであり、最上段のＫＲ（ルート鍵データ）から、最下段から２番目の節（ノード）に記載された鍵データ：ＫＲ～Ｋ１１１をノード鍵データとする。

図９に示すツリー構成において、例えばデバイス０はリーフ鍵データＫ０００００と、ノード鍵データ：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。

なお、図９のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図９のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。

さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図９に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図９の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。

例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはＣＤ等の

情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵データを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。

コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティテイは、図９の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図９のツリー中に複数存在する。

なお、ノード鍵データ、リーフ鍵データは、ある１つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノード鍵データ、リーフ鍵データは例えば鍵データの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行可能である。

このツリー構造において、図９から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はデバイスノード鍵データＤＮＫとして共通の鍵データＫ００、Ｋ０、ＫＲを含むデバイスノード鍵データＤＮＫを保有する。

このノード鍵データ共有構成を利用することにより、例えば共通の鍵データをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノード鍵データＫ００は、デバイス０，１，２，３に共通する保有鍵データとなる。

また、新たな鍵データＫｎｅｗをノード鍵データＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノード鍵データＫ００を用いて暗号Ｅｎｃ（Ｋ

００，Ｋｎｅｗ）を解いて新たな鍵データＫｎｅｗを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。

そのためには、ノード鍵データ：Ｋ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新鍵データを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新鍵データであることを示す。

更新鍵データの配布処理について説明する。鍵データの更新は、例えば、図１０（Ａ）に示す有効化鍵ブロックＥＫＢによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

なお、有効化鍵ブロックＥＫＢは、図９に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新された鍵データを配布するための暗号化鍵データによって構成される。有効化鍵ブロックＥＫＢは、鍵データ更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれることもある。

図１０（Ａ）に示す有効化鍵ブロックＥＫＢには、ノード鍵データの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。

図１０の例は、図９に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノード鍵データを配布することを目的として形成されたブロックデータである。

図９から明らかなように、デバイス０，デバイス１は、更新ノード鍵データと

してK（t）００、K（t）0、K（t）Rが必要であり、デバイス２は、更新ノード鍵データとしてK（t）００１、K（t）００、K（t）0、K（t）Rが必要である。

図１０（A）のＥＫＢに示されるようにＥＫＢには複数の暗号化鍵データが含まれる。最下段の暗号化鍵データは、Ｅｎｃ（K００１０，K（t）００１）である。これはデバイス２の持つリーフ鍵データK００１０によって暗号化された更新ノード鍵データK（t）００１であり、デバイス２は、自身の持つリーフ鍵データによってこの暗号化鍵データを復号し、K（t）００１を得ることができる。

また、復号により得たK（t）００１を用いて、図１０（A）の下から２段目の暗号化鍵データＥｎｃ（K（t）００１，K（t）００）を復号可能となり、更新ノード鍵データK（t）００を得ることができる。

以下順次、図１０（A）の上から２段目の暗号化鍵データＥｎｃ（K（t）００，K（t）0）を復号し、更新ノード鍵データK（t）0、図１０（A）の上から１段目の暗号化鍵データＥｎｃ（K（t）0，K（t）R）を復号しK（t）Rを得る。一方、デバイスK０００００．K０００１は、ノード鍵データK０００は更新する対象に含まれておらず、更新ノード鍵データとして必要なのは、K（t）００、K（t）0、K（t）Rである。

デバイスK０００００．K０００１は、図１０（A）の上から３段目の暗号化鍵データＥｎｃ（K０００，K（t）００）を復号しK（t）００、を取得し、以下、図１０（A）の上から２段目の暗号化鍵データＥｎｃ（K（t）００，K（t）0）を復号し、更新ノード鍵データK（t）0、図１０（A）の上から１段目の暗号化鍵データＥｎｃ（K（t）0，K（t）R）を復号しK（t）Rを得る。このようにして、デバイス０，１，２は更新した鍵K（t）Rを得ることができる。

なお、図１０（A）のインデックスは、復号鍵データとして使用するノード鍵

データ、リーフ鍵データの絶対番地を示す。

図９に示すツリー構造の上位段のノード鍵データ：Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノード鍵データＫ００のみの更新処理が必要である場合には、図１０（Ｂ）の有効化鍵ブロックＥＫＢを用いることで、更新ノード鍵データＫ（ｔ）００をデバイス０，１，２に配布することができる。

図１０（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツ鍵データを配布する場合に利用可能である。

具体例として、図９に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツ鍵データＫ（ｔ）ｃｏｎが必要であるとする。

このとき、デバイス０，１，２，３の共通のノード鍵データＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツ鍵データ：Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）を図１０（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点での鍵データ、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵データＫ（ｔ）ｃｏｎを得ることが可能になる。

図１１に、ｔ時点での鍵データ、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵データＫ（ｔ）ｃｏｎをＥＫＢの処理によって取得する処理例を示す。

ＥＫＢには、Ｋ（ｔ）００を用いてコンテンツ鍵データＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図１０（Ｂ）に示すデータとが格納されているとする。ここでは、デバイス０の処理例を示す。

図１１に示すように、デバイス０は、記録媒体に格納されている世代：ｔ 時点のＥＫＢと自分があらかじめ格納しているノード鍵データＫ０００を用いて上述

したと同様のＥＫＢ処理により、ノード鍵データＫ（ｔ）００を生成する。

さらに、復号した更新ノード鍵データＫ（ｔ）００を用いて暗号化データＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）を復号して更新コンテンツ鍵データＫ（ｔ）ｃｏｎを取得する。さらに、デバイスは、後にそれを使用するために自分だけが持つリーフ鍵データＫ００００で暗号化して格納してもよい。

また、別の例として、ツリー構造のノード鍵データの更新は不必要で、時点ｔでのコンテンツ鍵データＫ（ｔ）ｃｏｎのみを必要な機器が得られればよい、という場合もある。この場合、下記のような方式とすることができる。

いま、図１１の例と同様に、デバイス０、１、２にのみコンテンツ鍵データＫ（ｔ）ｃｏｎを送りたいとする。このとき、ＥＫＢは、

バージョン（Ｖｅｒｓｉｏｎ）：ｔ

インデックス　暗号化鍵データ

０００　　Ｅｎｃ（Ｋ０００、Ｋ（ｔ）ｃｏｎ）

００１０　　Ｅｎｃ（Ｋ００１０、Ｋ（ｔ）ｃｏｎ）

となる。

デバイス０、１はＫ０００を用いて、またデバイス２はＫ００１０を用いて上記ＥＫＢのうちの１つの暗号文を復号することによりコンテンツ鍵データを得ることができる。このようにすることにより、ノード鍵データの更新は行えないものの、必要な機器にコンテンツ鍵データを与える方法をより効率よく（すなわち、ＥＫＢに含まれる暗号文数を減らしてＥＫＢのサイズを小さくするとともに、管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

図１２に有効化鍵ブロックＥＫＢのフォーマット例を示す。バージョン６１は、有効化鍵ブロックＥＫＢのバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化鍵ブロックＥＫＢの配布先のデバイスに対する階層ツリーの階層数

を示す。データポインタ６３は、有効化鍵ブロックＥＫＢ中のデータ部の位置を示すポインタであり、タグポインタ６４はタグ部の位置、署名ポインタ６５は署名の位置を示すポインタである。

データ部６６は、例えば更新するノード鍵データを暗号化したデータを格納する。例えば図５に示すような更新されたノード鍵データに関する各暗号化鍵データ等を格納する。

タグ部６７は、データ部に格納された暗号化されたノード鍵データ、リーフ鍵データの位置関係を示すタグである。このタグの付与ルールを図１３を用いて説明する。

図１３では、データとして先に図１０（Ａ）で説明した有効化鍵ブロックＥＫＢを送付する例を示している。

この時のデータは、図１３の表（ｂ）に示すようになる。このときの暗号化鍵データに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルート鍵データの更新鍵データＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。

このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図１３の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図１３（ｃ）に示すデータ列、およびタグ列が構成される。

タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納される鍵データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）... は、単純に暗号化された鍵データの羅列データに

過ぎないので、上述したタグによってデータとして格納された暗号化鍵データのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図１０で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）

００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）

．．．のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。

これに対し、上述したタグを鍵データ位置を示す索引データとして用いることにより、少ないデータ量で鍵データ位置の判別が可能となる。

図１２に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）６８は、有効化鍵ブロックＥＫＢを発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化鍵ブロックＥＫＢ発行者が発行した有効化鍵ブロックＥＫＢであることを確認する。

ノード鍵データ等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的な鍵データ更新処理、暗号化鍵データ配信、データ配信を実行する構成について、以下説明する。

図１４は、階層ツリー構造のカテゴリの分類の一例を説明するための図である。

図１４において、階層ツリー構造の最上段には、ルート鍵データＫｒｏｏｔ７１が設定され、以下の中間段にはノード鍵データ７２が設定され、最下段には、リーフ鍵データ７３が設定される。各デバイスは個々のリーフ鍵データと、リーフ鍵データからルート鍵データに至る一連のノード鍵データ、ルート鍵データを

保有する。

ここで、一例として最上段から第M段目のあるノードをカテゴリノード７４として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の１つのノードを頂点として以下、M＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

例えば図１４の第M段目の１つのノード７５にはカテゴリＡが設定され、このノード以下に連なるノード、リーフはカテゴリＡに区分され、様々なデバイスを含むカテゴリＡ専用のノードまたはリーフとして設定される。すなわち、ノード７５以下を、カテゴリＡとして区分されるデバイスの関連ノード、およびリーフの集合として定義する。

さらに、M段から数段分下位の段をサブカテゴリノード７６として設定することができる。

例えば図に示すようにカテゴリＡノード７５の２段下のノードに、カテゴリＡに含まれるサブカテゴリＡａノードとして、[再生専用器] のノードを設定する。

さらに、サブカテゴリＡａノードである再生専用器のノード７６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード７７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［ＰＨＳ］ノード７８と［携帯電話］ノード７９を設定することができる。

さらに、カテゴリ、サブカテゴリは、デバイスの種類、メーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位で設定可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺにその頂点ノード以下の下段のノード鍵データ、リーフ鍵データを格納して販売することが可能となり、その後、暗号化コンテンツデータの配信、あるいは各種鍵データの配信、更新処理を、その頂点ノード鍵データ以下のノード鍵データ、リーフ鍵データによって

構成される有効化鍵ブロックＥＫＢを生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

また、コンテンツプロバイダの管理するノードをカテゴリノードとした場合には、コンテンツプロバイダが提供するコンテンツを格納したＣＤ、ＭＤ、ＤＶＤ等の情報記録媒体またはネット配信コンテンツを利用する機器をカテゴリノード以下に設定して、その機器に対してその頂点ノード以下の下段のノード鍵データ、リーフ鍵データを提供することが可能となる。

このように、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化鍵ブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずに鍵データ更新を実行することができる。

例えば、図１５に示されるように、ツリー構成のシステムで、鍵データ管理が行われる。

図１５の例では、８＋２４＋３２段のノードがツリー構造とされ、ルートノードから下位の８段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばフラッシュメモリなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

そして、このカテゴリノードのうちの１つのノードに、ライセンスを管理するシステムとして本システム（Ｔシステムと称する）が対応する。

すなわち、このＴシステムのノードよりさらに下の階層の２４段のノードに対応する鍵データが、ショップサーバ、ライセンスサーバ等の管理エンティテイとしてのサービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。

この例の場合、これにより、224（約１６メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の３２段の階層により、232（約４ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。

最下段の３２段のノードからＴシステムのノードまでのパス上の各ノードに対応する鍵データが、ＤＮＫを構成し、最下段のリーフに対応するＩＤがリーフＩＤとされる。

例えば、コンテンツを暗号化したコンテンツ鍵データは更新されたルート鍵データＫＲ’によって暗号化され、上位の階層の更新ノード鍵データは、その直近の下位の階層の更新ノード鍵データを用いて暗号化され、ＥＫＢ内に配置される。ＥＫＢにおける末端から１つ上の段の更新ノード鍵データはＥＫＢの末端のノード鍵データあるいはリーフ鍵データによって暗号化され、ＥＫＢ内に配置される。

ユーザデバイスは、サービスデータに記述されているＤＮＫのいずれかの鍵データを用いて、コンテンツデータとともに配布されるＥＫＢ内に記述されている直近の上位の階層の更新ノード鍵データを復号し、復号して得た鍵データを用いて、ＥＫＢ内に記述されているさらにその上の階層の更新ノード鍵データを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルート鍵データＫＲ’を得ることができる。

上述したように、ツリーのカテゴリ分類により、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化鍵ブロックＥＫＢを独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

〔再生装置１５〕

図１６は、図２に示す再生装置１５の構成図である。

図１６に示すように、再生装置１５は、例えば、入出力インタフェース８１、

ＭＰＥＧ(Moving Picture Experts Group)等の各種符号化データの生成および復号を実行するコーデック８２、Ａ／Ｄ・Ｄ／Ａコンバータ８４を備えた入出力インタフェース８３、暗号処理部８５、ＲＯＭ（Read Only Memory）８６、コントローラ８７、メモリ８８、並びにディスク型記録媒体２にアクセスするための記録媒体インタフェース８９を有し、これらがバス８０によって相互に接続されている。

入出力インタフェース８１は、ネットワーク等、外部から供給されるデジタル信号を受信し、バス８０上に出力するとともに、バス８０上のデジタル信号を受信し、外部に出力する。

コーデック８２は、バス８０を介して供給される例えばＭＰＥＧ符号化されたデータをデコードし、入出力インタフェース８３に出力するとともに、入出力インタフェース８３から供給されるデジタル信号をエンコードしてバス８０上に出力する。

入出力インタフェース８３は、コンバータ８４を内蔵している。

入出力インタフェース８３は、外部から供給されるアナログ信号を受信し、コンバータ８４でＡ／Ｄ(Analog Digital)変換することで、デジタル信号として、コーデック８２に出力するとともに、コーデック８２からのデジタル信号をコンバータ８４でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理部８５は、例えば、１チップのＬＳＩで構成され、バス８０を介して供給される例えばコンテンツ等のデジタル信号を暗号化し、または復号し、バス８０上に出力する構成を持つ。

なお、暗号処理部８５は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

ＲＯＭ８６は、例えば、再生装置ごとに固有の、あるいは複数の再生装置のグループごとに固有のデバイス鍵データであるリーフ鍵データと、複数の再生装置、

あるいは複数のグループに共有のデバイス鍵データであるノード鍵データを記憶している。

コントローラ８７は、メモリ８８に記憶されたプログラムＰＲＧ３（第５の発明のプログラム）を実行することで、再生装置１５の処理を統括して制御する。

すなわち、再生装置１５の機能（処理）は、プログラムＰＲＧ３によって規定される。なお、再生装置１５の機能の全部あるいは一部を、ハードウェアによって実現してもよい。

メモリ８８は、上述したリボケーションリストＤＩＲＬをディスク型記録媒体２から読み取りセキュアな状態で格納する。

例えば再生装置１５に設定されたＩＤに基づく暗号化を施してメモリに格納するなどにより耐タンパ性を保持したデータとして格納することが好ましい。このようにリボケーションリストＤＩＲＬは外部から消されたり、内容を改ざんされたり、古いバージョンのリストに入れ替えられることを容易に実行されないように格納する。

記録媒体インタフェース８９は、ディスク型記録媒体２にアクセスするために用いられる。

以下、図１６に示す再生装置１５の動作例を説明する。

図１７は図１６に示す再生装置１５の全体動作例を説明するためのフローチャート、図１８は図１７に示すステップＳＴ３２のディスクＩＤの検証処理を説明するためのフローチャート、図１９は図１７に示すステップＳＴ３８のコンテンツ再生を説明するためのフローチャートである。

ステップＳＴ３１：

再生装置１５は、所定のアクセス位置にディスク型記録媒体２がセットされると、記録媒体インタフェース８９を介して、ディスク型記録媒体２からディスクＩＤを読み出し、これをメモリ８８に格納する。

ステップＳＴ３２：

再生装置１５のコントローラ８７は、ステップＳＴ３１でメモリ８８に格納したディスクＩＤを読み出してその改竄の有無および正当性を検証する。

当該検証については、後に詳細に説明する。

ステップＳＴ３３：

コントローラ８７は、ステップＳＴ３２で上記ディスクＩＤが正当であると検証するとステップＳＴ３５の処理に進み、そうでない場合にはステップＳＴ３４に進む。

ステップＳＴ３４：

コントローラ８７は、ディスク型記録媒体２に記録されている暗号化コンテンツデータＥＣＯＮＴの復号および再生を停止（禁止）する。

ステップＳＴ３５：

コントローラ８７は、記録媒体インタフェース８９を介して、ディスク型記録媒体２からリボケーションリストＤＩＲＬを読み出す。

そして、コントローラ８７は、当該読み出したリボケーションリストＤＩＲＬの改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵（公開鍵）によって検証する。また、改竄検証値としてメッセージ認証コードＭＡＣが付与されている場合は、先に図８を参照して説明したＭＡＣ検証処理が実行される。

そして、コントローラ８７は、リボケーションリストＤＩＲＬに改竄がないと判定されたことを条件に、当該リボケーションリストＤＩＲＬのバージョンと、メモリ８８に既に格納されているリボケーションリストＤＩＲＬとのバージョン比較を実行する。

コントローラ８７は、当該読み出したリボケーションリストＤＩＲＬのバージョンがメモリ８８に既に格納されているリボケーションリストＤＩＲＬより新しい場合は、当該読み出したリボケーションリストＤＩＲＬによって、メモリ８８内のリボケーションリストＤＩＲＬを更新する。

ステップＳＴ３６：

コントローラ８７は、ステップＳＴ３１で読み出したディスクＩＤがリボケーションリストＤＩＲＬ内に存在するか否かを判断し、存在すると判断するとステップＳＴ３８に進み、そうでない場合にはステップＳＴ３７に進む。

ステップＳＴ３７：

コントローラ８７は、ディスク型記録媒体２に記録されている暗号化コンテンツデータＥＣＯＮＴの復号および再生を停止（禁止）する。

ステップＳＴ３８：

コントローラ８７は、ディスク型記録媒体２に記録されている暗号化コンテンツデータＥＣＯＮＴを読み出し、これを復号して再生する。

ステップＳＴ３８の処理については、後に詳細に説明する。

以下、図１７に示すディスクＩＤの検証（ＳＴ３２）について詳細に説明する。

図１８は、図１７に示すステップＳＴ３２を説明するためのフローチャートである。

図１８の処理が、第４の発明の工程に対応し、ステップＳＴ４２が第１の工程に対応し、ステップＳＴ４３～ＳＴ４６が第２の工程に対応している。

また、図１８の処理をコントローラ８７が行うことで、第６の発明の手段が実現される。

ステップＳＴ４１：

再生装置１５のコントローラ８７は、図１７に示すステップＳＴ３１で読み出したディスクＩＤ（w）内の署名データＳＩＧ（w）（第４～第６の発明の署名データ）を取り出す。

ステップＳＴ４２：

コントローラ８７は、メモリ８８から読み出した管理装置１２（管理局ＣＡ）の公開鍵データ（第４～第６の発明の公開鍵データ）および公開されたパラメータを基に、ステップＳＴ４１で読み出した署名データＳＩＧ（w）からメッセー

ジM（w）’（第４の発明の第１のデータ）を生成する。

ステップＳＴ４３：

コントローラ８７は、ディスクＩＤ（w）内のメッセージM（w）あるいはM（第４の発明の第２のデータ）と、ステップＳＴ４２で生成したメッセージM（w）’とを比較する。

ステップＳＴ４４：

コントローラ８７は、ステップＳＴ４３の比較で一致していると判定するとステップＳＴ４５に進み、そうでない場合にはステップＳＴ４６に進む。

ステップＳＴ４５：

コントローラ８７は、ステップＳＴ４１で取り出したディスクＩＤ（w）が正当であると判定する。

ステップＳＴ４６：

コントローラ８７は、ステップＳＴ４１で取り出したディスクＩＤ（w）が不正であると判定する。

以下、図１７に示すステップＳＴ３８の再生処理について説明する。

図１９は、図１７に示すステップＳＴ３８の再生処理を説明するためのフローチャートである。

ステップＳＴ５１：

再生装置１５は、記録媒体インタフェース８９を介して、ディスク型記録媒体２から暗号鍵情報、すなわち有効化鍵ブロックＥＫＢを読み出す。

ステップＳＴ５２：

コントローラ８７は、図１１を用いて前述したように、階層型鍵データ配信構成によって予め再生装置に提供されているデバイスノード鍵データＤＮＫに基づいて有効化鍵ブロックＥＫＢの復号処理を実行して、コンテンツ鍵データを取得する。

ステップＳＴ５３：

コントローラ８７は、記録媒体インタフェース８９を介して、ディスク型記録媒体２から暗号化コンテンツデータＥＣＯＮＴを読み出す。

ステップＳＴ５４：

コントローラ８７は、ステップＳＴ５２で取得したコンテンツ鍵データを用いて、ステップＳＴ５３で読み出した暗号化コンテンツデータＥＣＯＮＴを復号する。

ステップＳＴ５５：

コントローラ８７は、ディスク型記録媒体２に記録されている全ての暗号化コンテンツデータＥＣＯＮＴを復号したと判断すると、処理を終了し、そうでない場合にはステップＳＴ５３に戻る。

以上説明したように、コンテンツ提供システム１では、ディスク型記録媒体２に記録するディスクＩＤを、管理装置１２において、管理装置１２の秘密鍵データを基に署名データとして生成する。

また、再生装置１５において、ディスク型記録媒体２から読み出したディスクＩＤを、管理装置１２の公開鍵データを用いて検証する。

そのため、ディスク型記録媒体２に記録されてるディスクＩＤが改竄されたり、不正者によって生成された場合に、そのことを再生装置１５などが容易に検出できる。

その結果、不正に複製されたディスク型記録媒体２の流通を効果的に抑制することが可能になり、コンテンツ提供者の利益を保護できる。

上述したように、第１実施形態では、ディスクＩＤは任意の値ではなく、信頼できる機関である管理局ＣＡの管理装置１２が生成し、署名したものを用いた。

また、上述した第１実施形態では、コンテンツデータを暗号化して暗号化コンテンツデータＥＣＯＮＴを得るために用いたコンテンツ鍵データは、ディスクＩＤとは独立して生成されている。

以下に示す実施形態では、コンテンツ鍵データをディスクＩＤから導出する場

合を例示する。

これにより、不正者が、任意のディスクＩＤを用いて海賊版ディスクを無制限に製造する効果をさらに高めることができる。

＜第２実施形態＞

第２実施形態は、第７～第１２および第２６の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図４に示す管理装置１２によるディスクＩＤの生成処理、図１８に示すディスクＩＤの検証処理、図１９に再生処理におけるコンテンツ復号データの取得処理を除いて、第１実施形態のコンテンツ提供システム１と同じである。

本実施形態では、ディスクＩＤはディスクＩＤからタイトルごとに共通のメッセージＳを導出できるように生成され、このメッセージＳをコンテンツ鍵データとして用いる。

以下、本実施形態における管理装置１２ａのディスクＩＤ生成方法を説明する。

図２０は、本実施形態のコンテンツ提供システムにおいて管理装置１２ａが行うディスクＩＤの生成方法を説明するためのフローチャートである。

図２０に示す各処理は、コントローラ２７がプログラムＰＲＧ１ａを実行することによって実現され、この場合にプログラムＰＲＧ１ａが第８の発明に対応する。

また、コントローラ２７が図２０に示す各ステップを実行することで、第９の発明の第１の手段および第２の手段が実現される。この場合に、管理装置１２ａが第８および第９の発明のデータ処理装置に対応している。

なお、図２０に示す処理の全部または一部は、コントローラ２７がプログラムＰＲＧ１ａを実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

ステップＳＴ１０１：

管理装置１２ａのコントローラ２７は、デジタル署名のための鍵データ（管理

局ＣＡの公開鍵データおよび秘密鍵データ)、並びに署名生成および検証のためのパラメータを決定する。

コントローラ２７は、上記公開鍵データおよび上記パラメータを公開する。

当該公開は、例えば、コントローラ２７が、入出力インタフェース２４を介してネットワークを介して送信を行って実現する。

ステップＳＴ１０１の処理は、管理装置１２のセットアップ時に一度だけ行えばよい。

ステップＳＴ１０２：

管理装置１２は、入出力インタフェース２４を介して、コンテンツプロバイダから、コンテンツ（たとえば映画）のタイトルと，製造するディスクの枚数W（W≧２）を入力し、これをメインメモリ２２に格納する。

演算ユニット２６は、コンテンツデータのタイトルに対してメッセージＳ（第７～第９の発明のデータＳ）を決定する。

当該メッセージＳが後述する、ディスクＩＤから導出される値となり、コンテンツ鍵データとして用いられる。

ステップＳＴ１０３：

演算ユニット２６は、ステップＳＴ１０２で決定したメッセージＳと、乱数ｒ（w）と、上記パラメータとを用いて、W個のデジタルの異なる署名データＳＩＧ（w）を生成する。

ここで、w＝１，２・・・，Wであり，ｒ（w）はそれぞれ個別の乱数である。

ステップＳＴ１０４：

コントローラ２７は、w番目のディスクＩＤ（w）として、（Ｓ，ＳＩＧ（w））の組をタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置１４は、図６を用いて前述した手順で、上記ディスクＩＤ（w）を記録したディスク型記録媒体２ａ（第２６の発明の記録媒体）を製造する。

また、ディスク製造装置１４は、ステップＳＴ１０２で決定したメッセージＳを、コンテンツ鍵データとしてコンテンツデータを暗号化した暗号化コンテンツデータＥＣＯＮＴをディスク型記録媒体２ａに記録する。

以下、本実施形態における再生装置１５ａの動作例を説明する。

本実施形態の再生装置１５ａは、図１７に示すステップＳＴ３２およびステップＳＴ３８の処理のみが第１実施形態の場合と異なる。

図２１は、本実施形態における再生装置１５ａによるディスクＩＤの検証を説明するためのフローチャートである。

図２１に示す処理が第１０の発明の第１の工程に対応し、図２２に示す処理が第１０の発明の第２の工程に対応している。

また、コントローラ８７が図２１に示す処理を実行することで第１２の発明の第１の手段が実現され、図２２の処理を実行することで第１２の発明の第２の手段が実現される。

また、以下に示す処理は、再生装置１５ｂのコントローラ８７がプログラムＰＲＧ３ｃ（第１７の発明のプログラム）を実行して実現される。

ステップＳＴ１１１：

再生装置１５ａのコントローラ８７は、図１７に示すステップＳＴ３１で上述したディスク型記録媒体２ａから読み出したディスクＩＤ（ｗ）内の署名データＳＩＧ（ｗ）を取り出す。

ステップＳＴ１１２：

コントローラ８７は、メモリ８８から読み出した管理装置１２（管理局ＣＡ）の公開鍵データと公開されたパラメータとを基に、ステップＳＴ１１１で取り出した署名データＳＩＧ（ｗ）からメッセージＳ’（第１０～第１２の発明の第１のデータ）を生成する。

ステップＳＴ１１３：

コントローラ８７は、ディスクＩＤ（ｗ）内のメッセージＳ（第１０～第１２

の発明の第２のデータ）と、ステップＳＴ１１２で生成したメッセージＳ’とを比較する。

ステップＳＴ１１４：

コントローラ８７は、ステップＳＴ１１３の比較で一致していると判定するとステップＳＴ１１５に進み、そうでない場合にはステップＳＴ１１６に進む。

ステップＳＴ１１５：

コントローラ８７は、ステップＳＴ１１１で取り出したディスクＩＤ（w）が正当であると判定する。

ステップＳＴ１１６：

コントローラ８７は、ステップＳＴ１１１で取り出したディスクＩＤ（w）が不正であると判定する。

図２２は、本実施形態における図１７に示すステップＳＴ３８の再生処理を説明するためのフローチャートである。

本実施形態において、ステップＳＴ５１が無く、ステップＳＴ５２の代わりにステップＳＴ５２ａを行うこと以外は、図１９を用いて第１実施形態で説明したものと同じである。

ステップＳＴ５２ａ：

再生装置１５ａのコントローラ８７は、図２１の検証でディスクＩＤの正当性が認められたことを条件に、ディスクＩＤ（w）内のメッセージＳと再生装置１５ａが取得した図９を用いて説明したルート鍵データとを基にコンテンツ鍵データ（復号鍵）を生成する。コントローラ８７は、例えば、ルート鍵データと、メッセージＳとの排他的論理和をコンテンツ鍵データとする。

本実施形態のコンテンツ提供システムによっても、第１実施形態のコンテンツ提供システム１と同様の効果が得られる。

＜第３実施形態＞

第３実施形態は、第１３～第１８および第２７の発明に対応した実施形態であ

る。

本実施形態のコンテンツ提供システムは、図４に示す管理装置１２によるディスクＩＤの生成処理、図１８に示すディスクＩＤの検証処理、図１９に再生処理におけるコンテンツ復号データの取得処理を除いて、第１実施形態のコンテンツ提供システム１と同じである。

本実施形態では、ディスクＩＤはディスクＩＤからタイトルごとに共通のメッセージＳを導出できるように生成され、このメッセージＳをコンテンツ鍵データとして用いる。

以下、本実施形態における管理装置１２ｂのディスクＩＤ生成方法を説明する。

図２３は、本実施形態のコンテンツ提供システムにおいて管理装置１２ｂが行うディスクＩＤの生成方法を説明するためのフローチャートである。

図２３に示す各処理は、管理装置１２ｂのコントローラ２７がプログラムＰＲＧ１ｂを実行することによって実現され、この場合にプログラムＰＲＧ１ｂが第１４の発明に対応する。

また、コントローラ２７が図２３に示す各ステップを実行することで、第１５の発明の第１の手段および第２の手段が実現される。この場合に、管理装置１２ｂが第１４および第１５の発明のデータ処理装置に対応している。

なお、図２３に示す処理の全部または一部は、コントローラ２７がプログラムＰＲＧ１ｂを実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

ステップＳＴ２０１：

管理装置１２ｂのコントローラ２７が、ＲＳＡ暗号に用いるのに安全とされる程度に大きな素数ｑ１，ｑ２を選択する。

ステップＳＴ２０２：

コントローラ２７が、ステップＳＴ２０１で選択した素数ｑ１，ｑ２の積であるデータＭを公開する。

ステップＳＴ２０１，ＳＴ２０２の処理はシステムのセットアップ時に一度だけ行えばよい。

ステップＳＴ２０３：

コントローラ２７が、各タイトルに対して，Ｋ∈Ｚ＊Ｍ（Ｋは巡回群Ｚ＊Ｍの生成元）を満たすデータＫをランダムに選択する。

ここで、例えば、Ｘ∈Ｚ＊Ｍは、Ｘが、１～Ｘ－１の整数ｘのなかでｘを法として逆元を持つ集合の要素であることを示す。

ステップＳＴ２０４：

コントローラ２７が、コンテンツ製作者から，コンテンツのタイトルと製造するディスク型記録媒体２ｂ予定最大生産枚数Ｗを受け取る。

ステップＳＴ２０５：

コントローラ２７が、ステップＳＴ２０４の枚数Ｗに対応した数だけ、素数ｐ（ｗ）（ｗ＝１，２... Ｗ）を定める。例えば、ｗ番目の奇素数をｐ（ｗ）と定めてもよい。

ステップＳＴ２０６：

コントローラ２７が、そのタイトルに対応して、ディスクＩＤから導出される値をとして、データＳ（＝ＫＴ ｍｏｄＭ）を決定する。

但し、下記式（１）が成り立つ。

$$T = \prod_{w=1}^{W} Pw \quad \cdots (1)$$

ステップＳＴ２０７：

コントローラ２７が、（ＫＴ/ｐ(ｗ)ｍｏｄＭ）を演算して、その結果であるデータＩＤｋｅｙ（ｗ）を得る。

ステップＳＴ２０８：

コントローラ２７は、ｗ番目のディスクＩＤ（ｗ）として、ステップＳＴ２０

５で決定した素数ｐ（ｗ）と、ステップＳＴ２０７で得たデータＩＤｋｅｙ（ｗ）との組（ｐ（ｗ），ＩＤｋｅｙ（ｗ））をディスクＩＤとしてタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置１４は、図６を用いて前述した手順で、上記ディスクＩＤ（ｗ）を記録したディスク型記録媒体２ｂ（第２７の発明の記録媒体）を製造する。

また、ディスク製造装置１４は、上述したステップＳＴ２０６で決定したデータＳ（＝KT ｍｏｄM）をコンテンツ鍵データとしてコンテンツデータを暗号化して暗号化コンテンツデータＥＣＯＮＴを生成し、これをディスク型記録媒体２ｂに記録する。

以下、本実施形態における再生装置１５ｂの動作例を説明する。

本実施形態の再生装置１５ｂは、図１７に示すステップＳＴ３２およびステップＳＴ３８の処理のみが第１実施形態の場合と異なる。

図２４は、本実施形態における再生装置１５ｂによるディスクＩＤの検証を説明するためのフローチャートである。

図２４に示す処理が第１６の発明の第１の工程に対応している。

また、コントローラ８７が図２４に示す処理を実行することで第１８の発明の第１の手段が実現される。

また、以下に示す処理は、再生装置１５ｂのコントローラ８７がプログラムＰＲＧ３ｂ（第１７の発明のプログラム）を実行して実現される。

ステップＳＴ２１１：

再生装置１５ｂのコントローラ８７は、図１７に示すステップＳＴ３１で上述したディスク型記録媒体２ａから読み出したディスクＩＤ(w)内のデータｐ(w)を取り出す。

ステップＳＴ２１２：

コントローラ８７は、ステップＳＴ１１１で取り出したデータｐ（ｗ）が素数

か否かを判断する

コントローラ８７は、データｐ（ｗ）が素数であると判断するとステップＳＴ２１３に進み、そうでない場合にはステップＳＴ２１４に進む。

ステップＳＴ２１３：

コントローラ８７は、ステップＳＴ２１１で取り出したディスクＩＤ（ｗ）が正当であると判定する。

ステップＳＴ２１４：

コントローラ８７は、ステップＳＴ２１１で取り出したディスクＩＤ（ｗ）が不正であると判定する。

図２５は、本実施形態における図１７に示すステップＳＴ３８の再生処理を説明するためのフローチャートである。

図２５に示すステップＳＴ２２１が第１６の発明の第２の工程に対応し、ステップＳＴ２２４が第１６の発明の第３の工程に対応する。

また、コントローラ８７がステップＳＴ２２１を実行することで第１８の発明の第１の手段が実現され、ステップＳＴ２２４を実行することで第１８の発明の第２の手段が実現される。

ステップＳＴ２２１：

再生装置１５ｂのコントローラ８７は、記録媒体インタフェース８９を介して、ディスク型記録媒体２から読み出したデータｐ，ＩＤＫｅｙおよび公開されているデータＭを基に、（ＩＤｋｅｙｐｍｏｄＭ）を算出し、その結果をデータＳ’とする。

ステップＳＴ２２２：

コントローラ８７は、ステップＳＴ２２１で算出したデータＳ’と、再生装置１５ｂが取得した図９を用いて説明したルート鍵データとを基にコンテンツ鍵データ（復号鍵）を生成する。コントローラ８７は、例えば、ルート鍵データと、データＳ’との排他的論理和をコンテンツ鍵データとする。

ステップＳＴ２２３：

コントローラ８７は、記録媒体インタフェース８９を介して、ディスク型記録媒体２ｂから暗号化コンテンツデータＥＣＯＮＴを読み出す。

ステップＳＴ２２４：

コントローラ８７は、ステップＳＴ２２２のコンテンツ鍵データを用いて、ステップＳＴ２２３で読み出した暗号化コンテンツデータＥＣＯＮＴを復号する。

ステップＳＴ２２５：

コントローラ８７は、ディスク型記録媒体２ｂに記録されている全ての暗号化コンテンツデータＥＣＯＮＴを復号したと判断すると、処理を終了し、そうでない場合にはステップＳＴ２２３に戻る。

本実施形態のコンテンツ提供システムによっても、第１実施形態のコンテンツ提供システム１と同様の効果が得られる。

＜第４実施形態＞

第４実施形態は、第１９～第２４および第２８の発明に対応した実施形態である。

本実施形態のコンテンツ提供システムは、図４に示す管理装置１２によるディスクＩＤの生成処理、図１８に示すディスクＩＤの検証処理、図１９に再生処理におけるコンテンツ復号データの取得処理を除いて、第１実施形態のコンテンツ提供システム１と同じである。

以下、本実施形態における管理装置１２ｃのディスクＩＤ生成方法を説明する。

図２６は、本実施形態のコンテンツ提供システムにおいて管理装置１２ｃが行うディスクＩＤの生成方法を説明するためのフローチャートである。

図２６に示す各処理は、コントローラ２７がプログラムＰＲＧ１ｃを実行することによって実現され、この場合にプログラムＰＲＧ１ｃが第２０の発明に対応する。

また、コントローラ２７が図２６に示す各ステップを実行することで、第２１

の発明の第１の手段および第２の手段が実現される。この場合に、管理装置１２ｃが第２０および第２１の発明のデータ処理装置に対応している。

なお、図２６に示す処理の全部または一部は、コントローラ２７がプログラムＰＲＧ１ｃを実行する形態ではなく、同じ機能を実現する回路などのハードウェアによって実現してもよい。

ステップＳＴ３０１：

管理装置１２ｃのコントローラ２７が、ＲＳＡ暗号に用いるのに安全とされる程度に大きな素数ｑ１，ｑ２を選択する。

ステップＳＴ３０２：

コントローラ２７が、ステップＳＴ３０１で選択した素数ｑ１，ｑ２の積であるデータＭを公開する。

ステップＳＴ３０１，ＳＴ３０２の処理はシステムのセットアップ時に一度だけ行えばよい。

ステップＳＴ３０３：

コントローラ２７が、各タイトルに対して，Ｓ∈Ｚ＊Ｍ（Ｓは巡回群Ｚ＊Ｍの生成元）を満たすデータＳをランダムに選択する。当該データＳがディスクＩＤから導出される値となる。

ステップＳＴ３０４：

コントローラ２７が、コンテンツ製作者から，コンテンツのタイトルと製造するディスク型記録媒体２ｂ予定最大生産枚数Ｗを受け取る。

ステップＳＴ３０５：

コントローラ２７が、ｅ（ｗ）∈Ｚ＊Ｍ（ｅ（ｗ）は巡回群Ｚ＊Ｍの生成元）を満たす互いに異なるデータｅ（ｗ）選択する。

ここで、ｅ（ｗ）とλ（Ｍ）とは互いに素、すなわち、ｅ（ｗ）とλ（Ｍ）の最大公約数が１となる。なお、λ（Ｍ）は素数（ｑ１－１）と（ｑ２－１）との最少公倍数である。

ステップＳＴ３０６：

コントローラ２７が、（Ｓｄ(ｗ)ｍｏｄＭ）を演算して、その結果であるデータＩ（ｗ）を得る。

ここで、ｄ（ｗ）は、上記λ（Ｍ）を法としたときの上記ｅ（ｗ）の逆数である。すなわち、ｄ（ｗ）＝ｅ（ｗ）-1ｍｏｄλ（Ｍ）となる。

ステップＳＴ３０７：

コントローラ２７は、ｗ番目のディスクＩＤ（ｗ）として、ステップＳＴ３０５で決定したデータｅ（ｗ）と、ステップＳＴ３０６で得たデータＩ（ｗ）との組（ｅ（ｗ），Ｉ（ｗ））をディスクＩＤ（ｗ）としてタイトルとともにディスク製造者に提供する。

ディスク製造者のディスク製造装置１４は、図６を用いて前述した手順で、上記ディスクＩＤ（ｗ）を記録したディスク型記録媒体２ｃ（第２８の発明の記録媒体）を製造する。

また、ディスク製造装置１４は、上述したステップＳＴ３０３で選択したデータＳをコンテンツ鍵データとしてコンテンツデータを暗号化して暗号化コンテンツデータＥＣＯＮＴを生成し、これをディスク型記録媒体２ｃに記録する。

以下、本実施形態における再生装置１５ｃの動作例を説明する。

図２７は、再生装置１５ｃの動作例を説明するための図である。

図２７に示すステップＳＴ３１２が第２２の発明の第１の工程に対応し、ステップＳＴ３１６が第２２の発明の第２の工程に対応する。

また、コントローラ８７がステップＳＴ３１２を実行することで第２４の発明の第１の手段が実現され、ステップＳＴ３１６を実行することで第２４の発明の第２の手段が実現される。

また、図２７に示す各ステップは、再生装置１５ｃのコントローラ８７が、プログラムＰＲＧ３ｃ(第２３の発明のプログラム)を実行することで実現される。

ステップＳＴ３１１：

再生装置１５ｃは、所定のアクセス位置にディスク型記録媒体２ｃがセットされると、記録媒体インタフェース８９を介して、ディスク型記録媒体２ｃからディスクＩＤを読み出し、これをメモリ８８に格納する。

ステップＳＴ３１２：

再生装置１５ｃのコントローラ８７は、メモリ８８に記録したディスクＩＤ内のデータｅ（ｗ）とＩ（ｗ）とを用いて、Ｉ（ｗ）ｅ(ｗ)ｍｏｄＭを算出し、その結果をデータＳ’とする。

ステップＳＴ３１３：

コントローラ８７は、記録媒体インタフェース８９を介して、ディスク型記録媒体２ｃからリボケーションリストＤＩＲＬを読み出す。

そして、コントローラ８７は、当該読み出したリボケーションリストＤＩＲＬの改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵（公開鍵）によって検証する。また、改竄検証値としてメッセージ認証コードＭＡＣが付与されている場合は、先に図８を参照して説明したＭＡＣ検証処理が実行される。

そして、コントローラ８７は、リボケーションリストＤＩＲＬに改竄がないと判定されたことを条件に、当該リボケーションリストＤＩＲＬのバージョンと、メモリ８８に既に格納されているリボケーションリストＤＩＲＬとのバージョン比較を実行する。

コントローラ８７は、当該読み出したリボケーションリストＤＩＲＬのバージョンがメモリ８８に既に格納されているリボケーションリストＤＩＲＬより新しい場合は、当該読み出したリボケーションリストＤＩＲＬによって、メモリ８８内のリボケーションリストＤＩＲＬを更新する。

ステップＳＴ３１４：

コントローラ８７は、ステップＳＴ３１１で読み出したディスクＩＤがリボケーションリストＤＩＲＬ内に存在するか否かを判断し、存在すると判断するとス

テップＳＴ３１５に進み、そうでない場合にはステップＳＴ３１６に進む。

ステップＳＴ３１５：

コントローラ８７は、ディスク型記録媒体２ｃに記録されている暗号化コンテンツデータＥＣＯＮＴの再生を停止（禁止）する。

ステップＳＴ３１６：

コントローラ８７は、ディスク型記録媒体２ｃに記録されている暗号化コンテンツデータＥＣＯＮＴを読み出し、ステップＳＴ３１２で生成したデータＳ’を基に取得したコンテンツ鍵データを用いて、暗号化コンテンツデータＥＣＯＮＴを復号し、続いて再生する。

コントローラ８７は、例えば、ルート鍵データと、データＳ’との排他的論理和をコンテンツ鍵データとする。

本実施形態のコンテンツ提供システムによっても、第１実施形態のコンテンツ提供システム１と同様の効果が得られる。

本発明によれば、識別データを基に記録媒体を管理する場合に、その識別データを不正に生成並びに改竄することが困難な形態で生成できるデータ処理方法、そのプログラムおよびその装置を提供することができるという第１の効果が得られる。

また、本発明によれば、上記第１の効果を得るデータ処理方法、そのプログラムおよびその装置によって生成された識別データを適切に検証できるデータ処理方法、そのプログラムおよびその装置を提供することができるという第２の効果が得られる。

また、本発明によれば、上記第１の効果を得るデータ処理方法、そのプログラムおよびその装置によって生成された識別データを記録した記録媒体を提供できるという第３の効果が得られる。

産業上の利用可能性

本発明は、記録媒体を識別する識別データに係わる処理を行うデータ処理システムに利用可能である。

請 求 の 範 囲

1．記録媒体を識別する識別データを生成するデータ処理方法であって、

前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第１の工程と、

前記第１の工程で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第２の工程と

を有するデータ処理方法。

2．前記第１の工程において、複数の異なる第１のデータの各々について、当該第１のデータと、前記秘密鍵データと、所定の第２のデータとを用いて、前記秘密鍵データに対応する公開鍵データを基に前記第２のデータを生成可能な前記複数の署名データを生成し、

前記第２の工程において、前記第１の工程で生成した前記複数の署名データの各々について、当該署名データと前記第２のデータとを含む前記識別データを生成し、当該識別データを前記記録媒体に割り当てる

請求項１に記載のデータ処理方法。

3．　記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第１の手順と、

前記第１の手順で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第２の手順と

を有するプログラム。

4．　記録媒体を識別する識別データを生成するデータ処理装置であって、

前記識別データの管理元の秘密鍵データを用いて、複数の異なる署名データを生成する第１の手段と、

前記第１の手段で生成した前記複数の署名データを、前記識別データとして異なる複数の記録媒体にそれぞれ割当てる第２の手段と

を有するデータ処理装置。

５．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する工程

を有するデータ処理方法。

６．　前記工程は、

前記識別データに含まれる前記署名データから、前記公開鍵データを用いて第１のデータを生成する第１の工程と、

前記識別データに含まれる第２のデータと、前記第１の工程で生成した前記第１のデータとを比較し、当該比較の結果を基に、前記識別データの正当性を検証する第２の工程と

を有する請求項５に記載のデータ処理方法。

７．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手順

を有するプログラム。

８．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データの管理元の公開鍵データを用いて、前記識別データの正当性を検証する手段

を有するデータ処理装置。

９．　記録媒体を識別する識別データを生成するデータ処理方法であって、

前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する第１の工程と、

前記第１の工程で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第２の工程と

を有するデータ処理方法。

１０．　前記データＳを暗号化鍵として暗号化した暗号データと、前記識別データとを前記記録媒体に書き込む第３の工程

をさらに有する請求項９に記載のデータ処理方法。

１１．　記録媒体を識別する識別データを生成するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する第１の手順と、

前記第１の手順で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを異なる複数の記録媒体にそれぞれ割当てる第２の手順と

を有するプログラム。

１２．　記録媒体を識別する識別データを生成するデータ処理装置であって、

前記識別データの管理元の秘密鍵データとデータＳとを用いて、前記管理元の公開鍵データを基に前記データＳを復号可能な複数の異なる署名データを生成する第１の手段と、

前記第１の手段で生成した前記複数の署名データの各々について、当該署名データと前記データＳとを含む識別データを生成し、複数の前記識別データを

異なる複数の記録媒体にそれぞれ割当てる第２の手段と

を有するデータ処理装置。

１３．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する第１の工程と、

前記第１の工程で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する第２の工程と

を有するデータ処理方法。

１４．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する第１の手順と、

前記第１の手順で前記識別データが正当であると検証した場合に、前記記録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する第２の手順と

を有するプログラム。

１５．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データの管理元の公開鍵データを用いて前記識別データ内の署名データから第１のデータを生成し、当該第１のデータと前記識別データ内の第２のデータとを比較して前記識別データの正当性を検証する第１の手段と、

前記第１の手段で前記識別データが正当であると検証した場合に、前記記

録媒体から読み出した暗号データを、前記識別データ内の前記第２のデータを用いて復号する第２の手段と

を有するデータ処理装置。

１６．　公開されたデータＭを２つの素数の積とし、ＴをＷ（Ｗ≧２）個の異なる素数ｐ（ｗ）の積とし、ｗを１≦ｗ≦Ｗの整数とし、Ｋを巡回群Ｚ＊Ｍの生成元とした場合に、Ｗ 個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理方法であって、

（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する第１の工程と、

ｐ（ｗ）と前記第１の工程で算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の工程と

を有するデータ処理方法。

１７．　（ＫＴ　ｍｏｄＭ）を暗号化鍵として暗号化した暗号データと、前記識別データＩＤ（ｗ）とを前記記録媒体ＳＴＭ（ｗ）に書き込む第３の工程をさらに有する請求項１６に記載のデータ処理方法。

１８．　公開されたデータＭを２つの素数の積とし、ＴをＷ（Ｗ≧２）個の異なる素数ｐ（ｗ）の積とし、ｗを１≦ｗ≦Ｗの整数とし、Ｋを巡回群Ｚ＊Ｍの生成元とした場合に、Ｗ 個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置が実行するプログラムであって、

（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する第１の手順と、

ｐ（ｗ）と前記第１の手順で算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の手順と

を有するプログラム。

１９．　公開されたデータＭを２つの素数の積とし、ＴをＷ（Ｗ≧２）個の異なる素数ｐ（ｗ）の積とし、ｗを１≦ｗ≦Ｗの整数とし、Ｋを巡回群Ｚ＊Ｍの生成元とした場合に、Ｗ 個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置であって、

（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）を算出する第１の手段と、

ｐ（ｗ）と前記第１の手段が算出した（ＫＴ／ｐ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の手段と

を有するデータ処理装置。

２０．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データに含まれるデータｐが素数であるか否かを検証する第１の工程と、

前記第１の工程で前記データｐが素数であると検証された場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて　（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する第２の工程と、

前記第２の工程で算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第３の工程と

を有するデータ処理方法。

２１．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データに含まれるデータｐが素数であるか否かを検証する第１の手順と、

前記第１の手順で前記データｐが素数であると検証された場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する第２の手順と、

前記第２の手順で算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第３の手順と

を有するプログラム。

２２．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データに含まれるデータｐが素数であるか否かを検証する第１の手段と、

前記第１の手段が前記データｐが素数であると検証した場合に、前記識別データに含まれるデータＩＤＫｅｙと前記データｐと公開されているデータＭと用いて（ＩＤＫｅｙｐ　ｍｏｄＭ）を算出する第２の手段と、

前記第２の手段が算出した（ＩＤＫｅｙｐ　ｍｏｄＭ）を基に得た復号鍵を用いて、前記記録媒体に記録された暗号データを復号する第３の手段と

を有するデータ処理装置。

２３．　素数ｑ１とｑ２の積であり公開されたデータをＭとし、ｗを１≦ｗ≦Ｗ の整数とし、Ｗ（Ｗ≧２）個の異なるデータをｅ（ｗ）とし、ｅ（ｗ）を巡回群Ｚ＊Ｍの生成元とし、ｅ(ｗ)とλ（Ｍ）は互い素であり、λ（Ｍ）を（ｑ１－１）と（ｑ２－１）との最小公倍数とした場合に、Ｗ個の記録媒体ＳＴＭ（ｗ）の各々に割当てる識別データＩＤ（ｗ）を生成するデータ処理方法であって、

巡回群Ｚ＊Ｍの生成元であるデータＳと、λ(Ｍ)を法としたときのｅ（ｗ）の逆数であるデータｄ（ｗ）と、上記データＭとを用いて、（Ｓｄ(ｗ)　ｍｏｄＭ）を算出する第１の工程と、

前記ｅ（ｗ）と前記第１の工程で算出した（Ｓｄ（ｗ）　ｍｏｄＭ）とを含む識別データＩＤ（ｗ）を、記録媒体ＳＴＭ（ｗ）に割当てる第２の工程と

を有するデータ処理方法。

２４．　上記データＳを暗号鍵として用いて暗号化された暗号データと、前記識別データＩＤ（ｗ）とを前記記録媒体ＳＴＭ（ｗ）に書き込む第３の工程をさらに有する請求項２３に記載のデータ処理方法。

２５．　素数ｑ１とｑ２の積であり公開されたデータをＭとし、ｗを１≦ｗ≦Ｗ の整数とし、Ｗ（Ｗ≧２）個の異なるデータをｅ（ｗ）とし、ｅ（ｗ）を巡回群Ｚ＊Ｍの生成元とし、ｅ(ｗ)とλ（Ｍ）は互い素であり、λ（Ｍ）を（ｑ１－１）と（ｑ２－１）との最小公倍数とした場合に、Ｗ個の記録媒体ＳＴＭ（ｗ）の各々

に割当てる識別データＩＤ（ｗ）を生成するデータ処理装置が実行するプログラムであって、

巡回群Ｚ＊Ｍの生成元であるデータＳと、λ(Ｍ)を法としたときのｅ(ｗ)の逆数であるデータｄ(ｗ)と、上記データＭとを用いて、(Ｓｄ(ｗ)　ｍｏｄＭ)を算出する第１の手順と、

前記ｅ(ｗ)と前記第１の手順で算出した(Ｓｄ(ｗ)　ｍｏｄＭ)とを含む識別データＩＤ(ｗ)を、記録媒体ＳＴＭ(ｗ)に割当てる第２の手順と

を有するプログラム。

２６．　素数ｑ１とｑ２の積であり公開されたデータをＭとし、ｗを１≦ｗ≦Ｗ の整数とし、Ｗ(Ｗ≧２)個の異なるデータをｅ(ｗ)とし、ｅ(ｗ)を巡回群Ｚ＊Ｍの生成元とし、e(w)とλ(Ｍ)は互い素であり、λ(Ｍ)を(ｑ１－１)と(ｑ２－１)との最小公倍数とした場合に、Ｗ個の記録媒体ＳＴＭ(ｗ)の各々に割当てる識別データＩＤ(ｗ)を生成するデータ処理装置であって、

巡回群Ｚ＊Ｍの生成元であるデータＳと、λ(Ｍ)を法としたときのｅ(ｗ)の逆数であるデータｄ(ｗ)と、上記データＭとを用いて、(Ｓｄ(ｗ)　ｍｏｄＭ)を算出する第１の手段と、

前記ｅ(ｗ)と前記第１の手段が算出した(Ｓｄ(ｗ)　ｍｏｄＭ)とを含む識別データＩＤ(ｗ)を、記録媒体ＳＴＭ(ｗ)に割当てる第２の手段と

を有するデータ処理装置。

２７．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理方法であって、

前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて(Ｉｅ　ｍｏｄＭ)を算出する第１の工程と、

前記第１の工程で算出した(Ｉｅ　ｍｏｄＭ)を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第２の工程と

を有するデータ処理方法。

２８．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置が実行するプログラムであって、

前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ　ｍｏｄＭ）を算出する第１の手順と、

前記第１の手順で算出した（Ｉｅ　ｍｏｄＭ）を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第２の手順と

を有するプログラム。

２９．　記録媒体に割当てられた当該記録媒体を識別する識別データの正当性を検証するデータ処理装置であって、

前記識別データに含まれるデータｅおよびデータＩと公開されているデータＭと用いて（Ｉｅ　ｍｏｄＭ）を算出する第１の手段と、

前記第１の手が算出した（Ｉｅ　ｍｏｄＭ）を復号鍵として用いて、前記記録媒体に記録された暗号データを復号する第２の手段と

を有するデータ処理装置。

３０．　データを記録する記録媒体であって、

前記記録媒体の管理元の秘密鍵データを用いて生成され、前記管理元の公開鍵データを基に正当性が検証され、当該記録媒体を識別する識別データを記録した

記録媒体。

３１．　データを記録する記録媒体であって、

前記記録媒体の管理元の公開鍵データを用いて第１のデータを生成するために用いられる署名データと、前記第１のデータと比較して識別データの正当性を検証するために用いられる第２のデータとを含み前記記録媒体を識別する前記識別データを記録した

記録媒体。

３２．　暗号データを記録する記録媒体であって、

素数であるデータｐと、

前記暗号データを復号するために用いられるコンテンツ鍵データである（ＩＤＫｅｙｐ　ｍｏｄＭ）を前記データｐと公開されているデータＭと共に算出するために用いられるデータＩＤＫｅｙと

を含み前記記録媒体を識別する識別データを記録した

記録媒体。

３３．　暗号データを記録する記録媒体であって、

前記暗号データを復号するために用いられるコンテンツ鍵データである（Ｉｅ　ｍｏｄＭ）を、公開されているデータＭと共に算出するために用いられるデータｅおよびデータＩとを含み前記記録媒体を識別する識別データを記録した

記録媒体。

FIG. 1

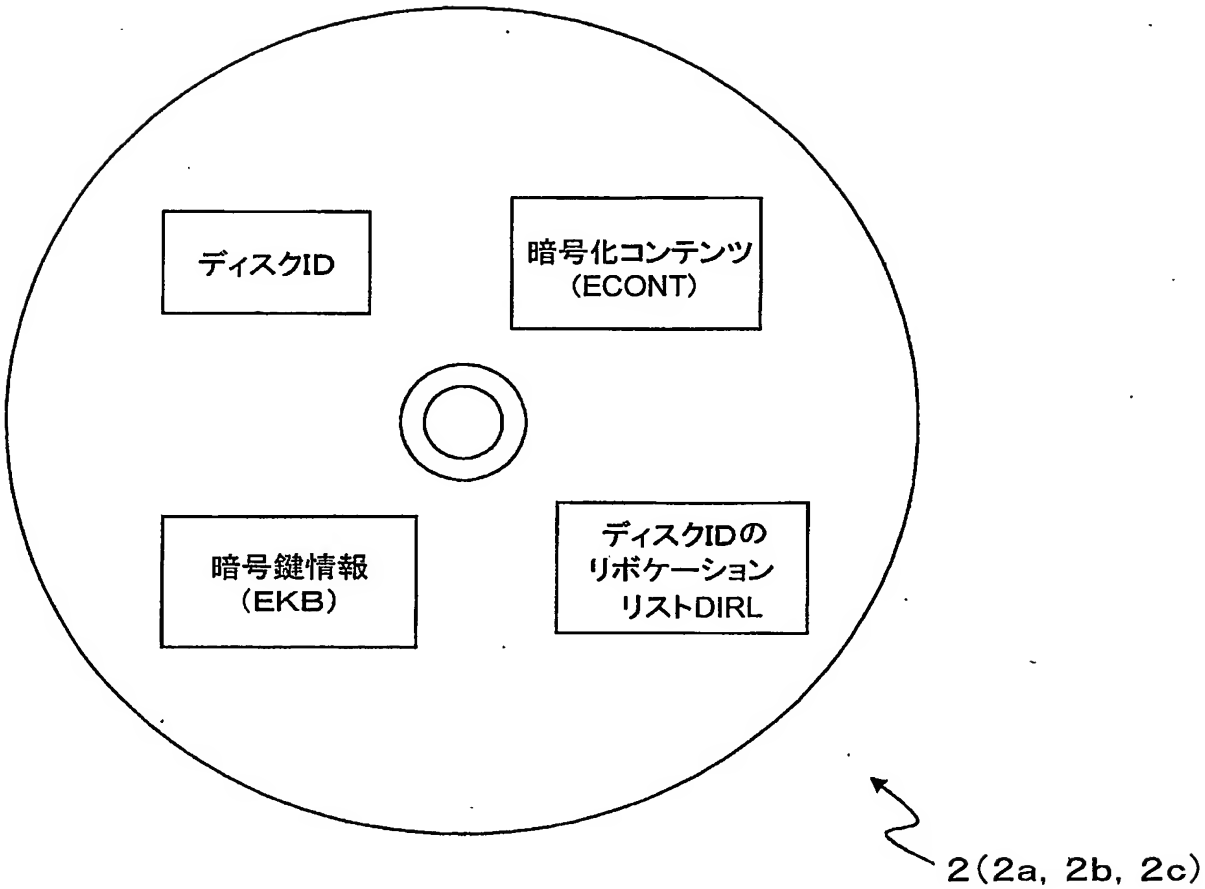

ディスクID
暗号化コンテンツ
(ECONT)
暗号鍵情報
(EKB)
ディスクIDの
リボケーション
リストDIRL
2(2a, 2b, 2c)

FIG. 2

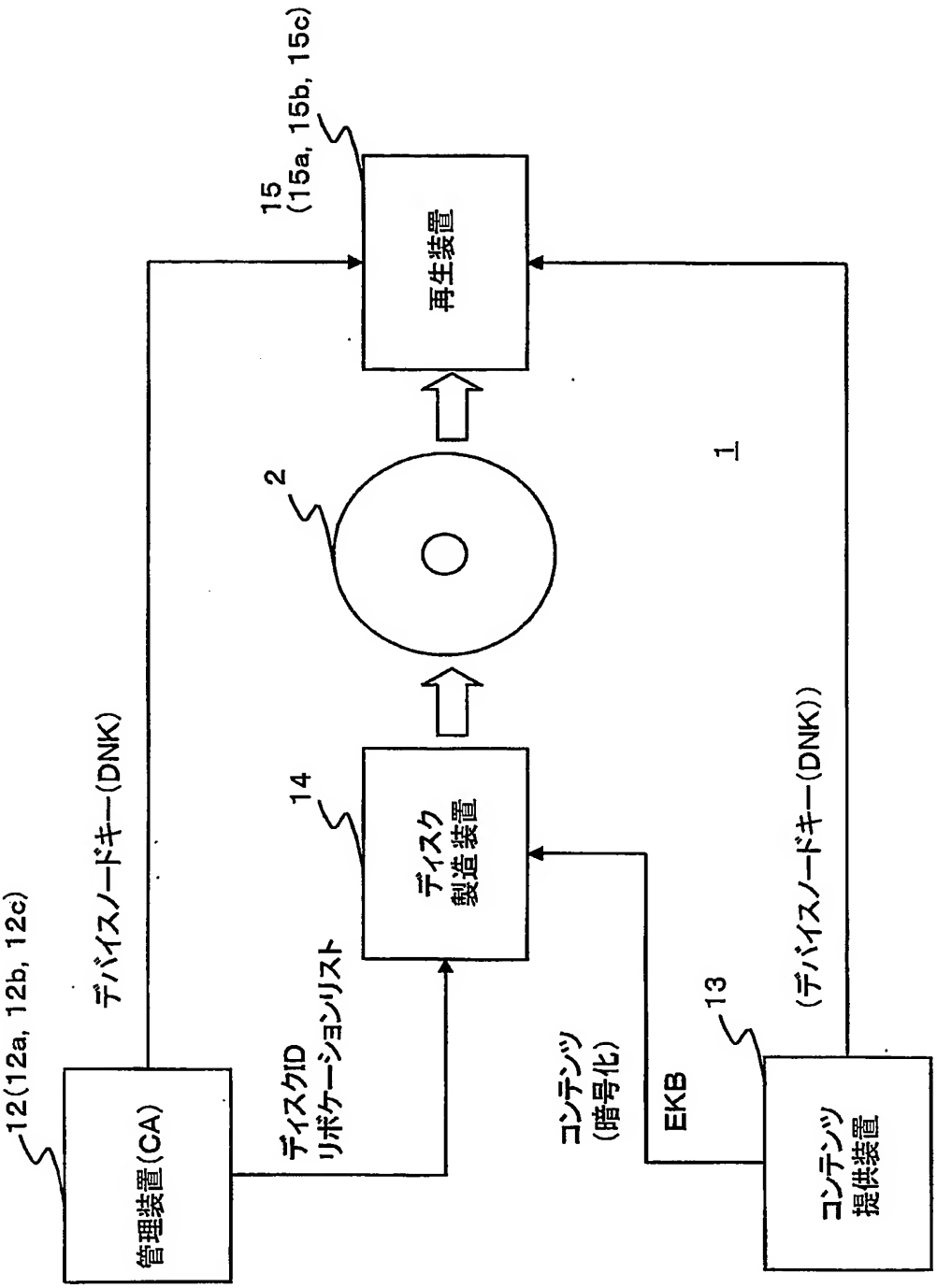

12(12a, 12b, 12c)
管理装置(CA)
デバイスノードキー(DNK)
ディスクID
リボケーションリスト
14
ディスク
製造装置
コンテンツ
(暗号化)
EKB
13
コンテンツ
提供装置
(デバイスノードキー(DNK))
2
15
(15a, 15b, 15c)
再生装置
1

FIG. 3

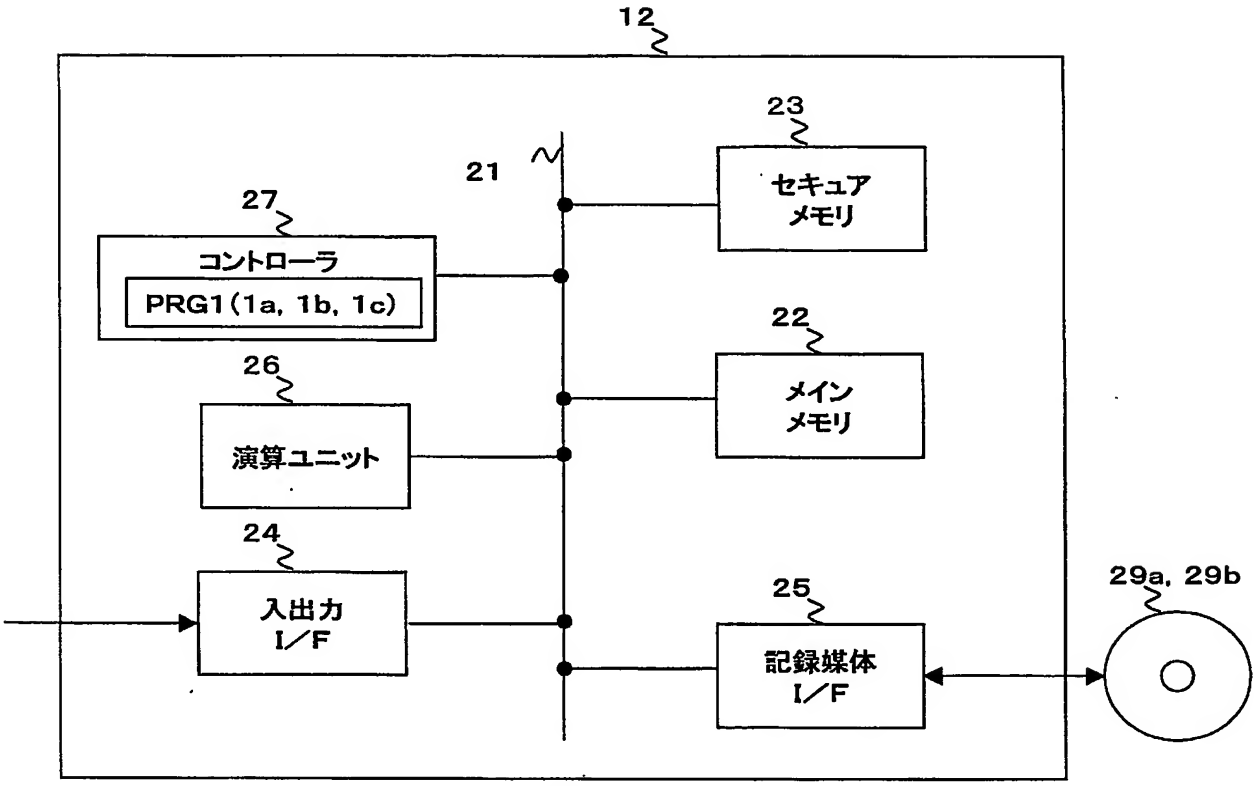

12
23
21
セキュア
メモリ
27
コントローラ
PRG1(1a, 1b, 1c)
22
メイン
メモリ
26
演算ユニット
24
入出力
I/F
25
29a, 29b
記録媒体
I/F

FIG. 4

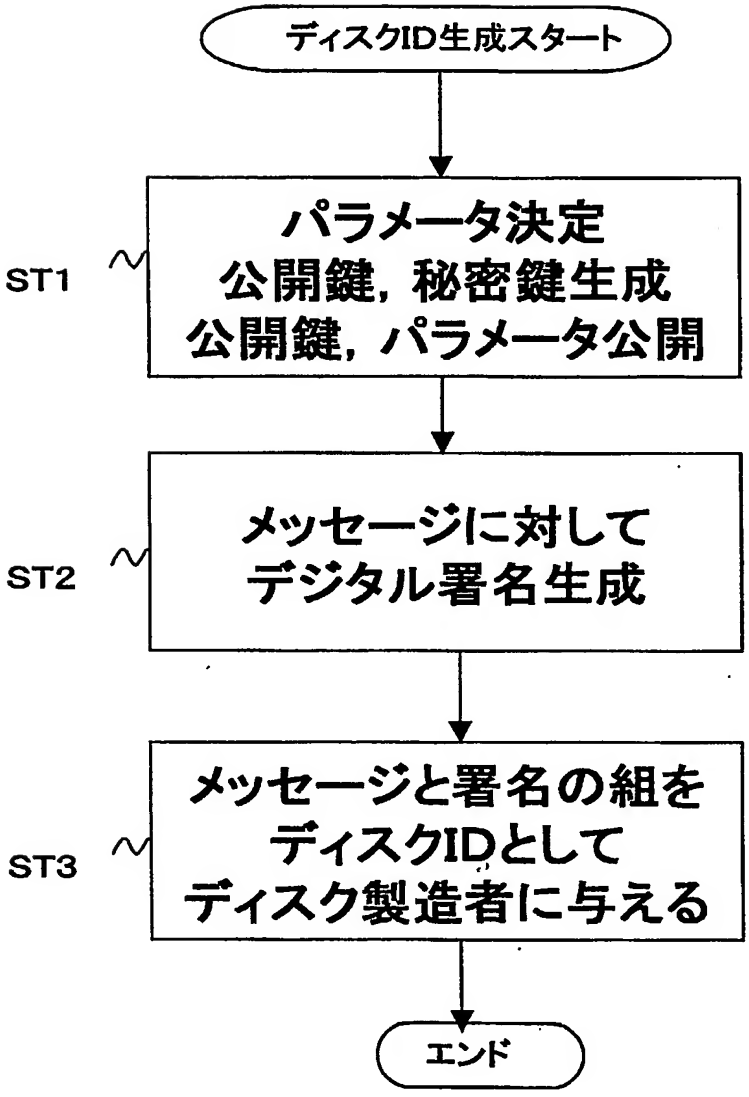

ディスクID生成スタート
ST1
パラメータ決定
公開鍵，秘密鍵生成
公開鍵，パラメータ公開
ST2
メッセージに対して
デジタル署名生成
ST3
メッセージと署名の組を
ディスクIDとして
ディスク製造者に与える
エンド
12

FIG. 5

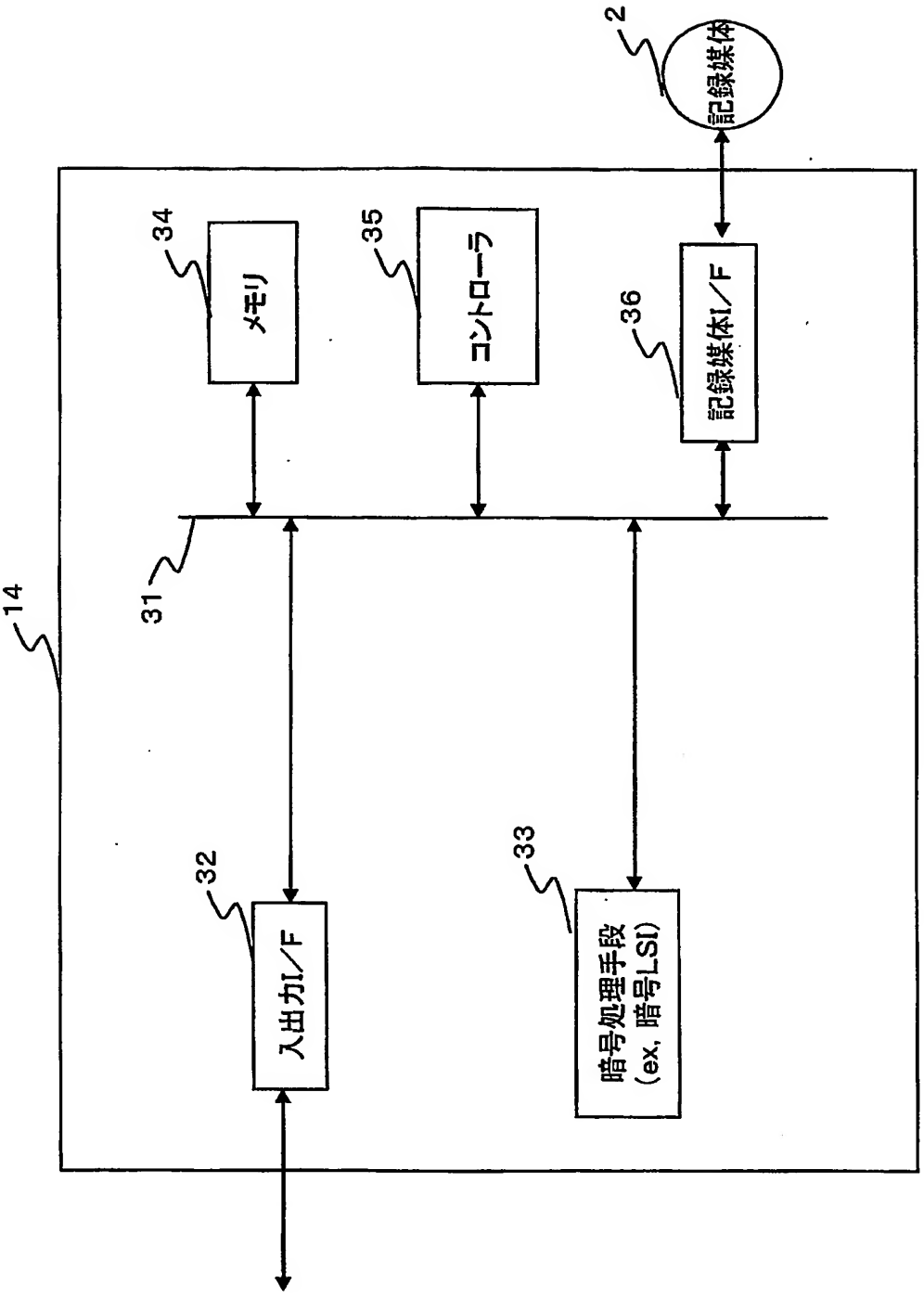

2
記録媒体
14
31
34
メモリ
35
コントローラ
36
記録媒体I／F
32
入出力I／F
33
暗号処理手段
(ex, 暗号LSI)

FIG. 6

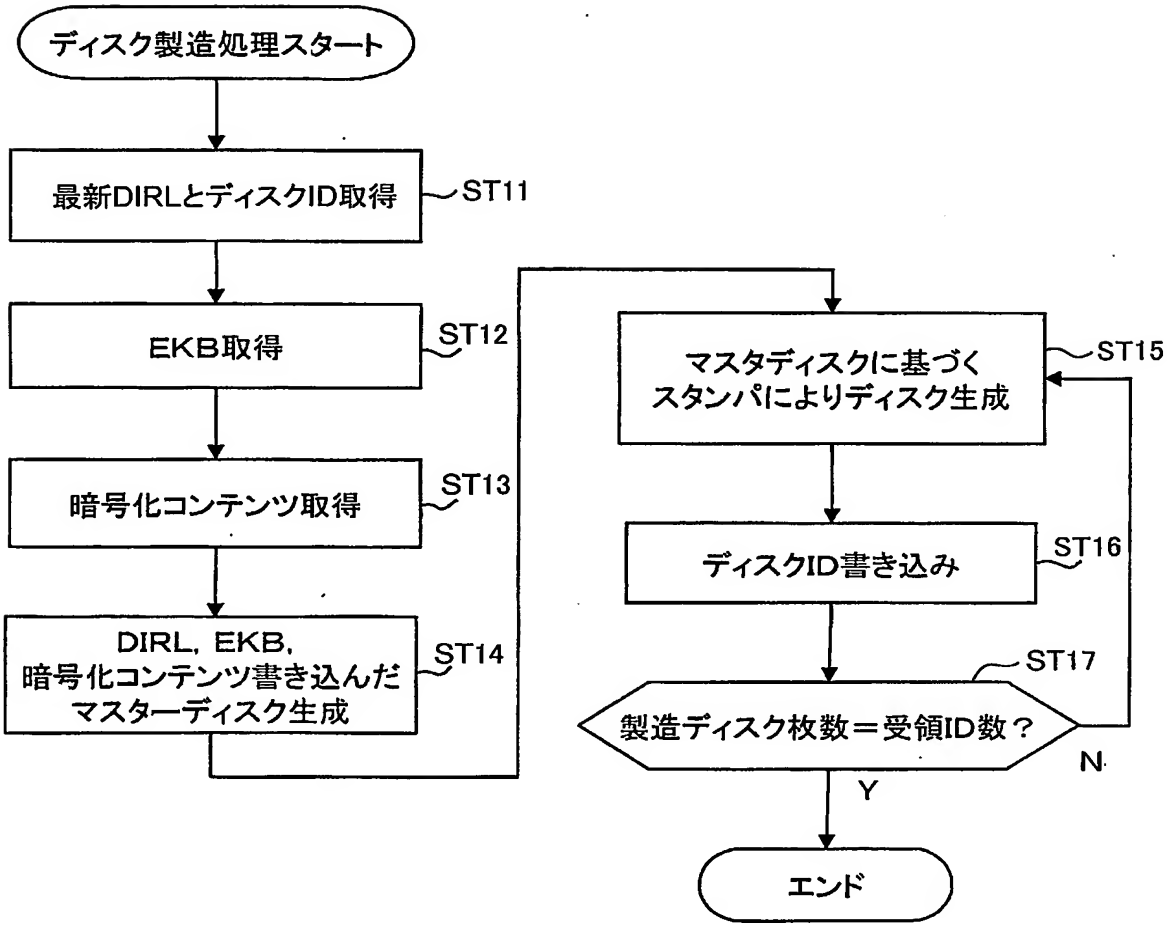

ディスク製造処理スタート
最新DIRLとディスクID取得
ST11
EKB取得
ST12
暗号化コンテンツ取得
ST13
DIRL, EKB,
暗号化コンテンツ書き込んだ
マスターディスク生成
ST14
マスタディスクに基づく
スタンパによりディスク生成
ST15
ディスクID書き込み
ST16
ST17
製造ディスク枚数＝受領ID数？
N
Y
エンド

FIG. 7

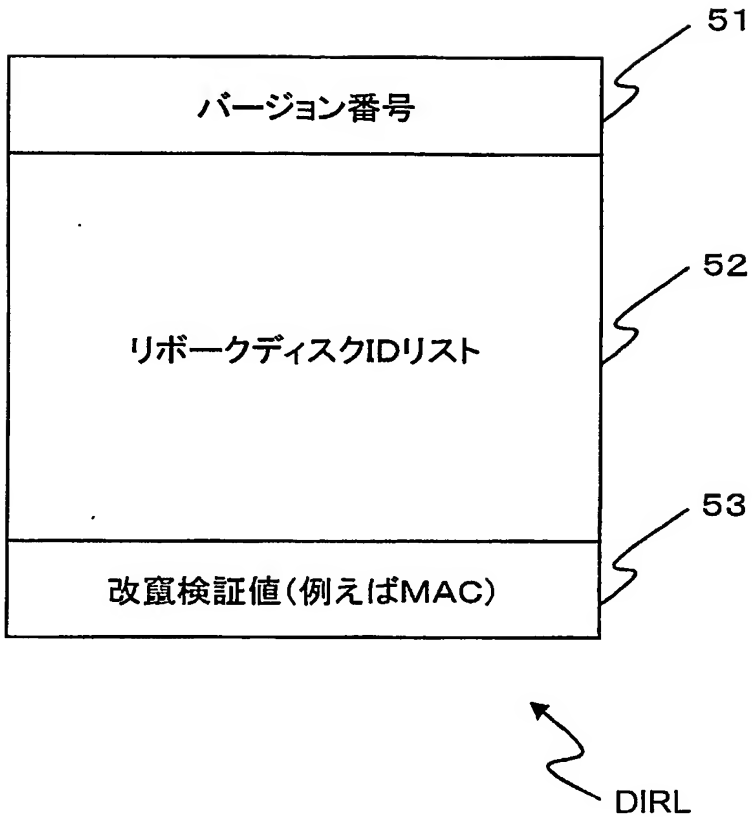


FIG. 8

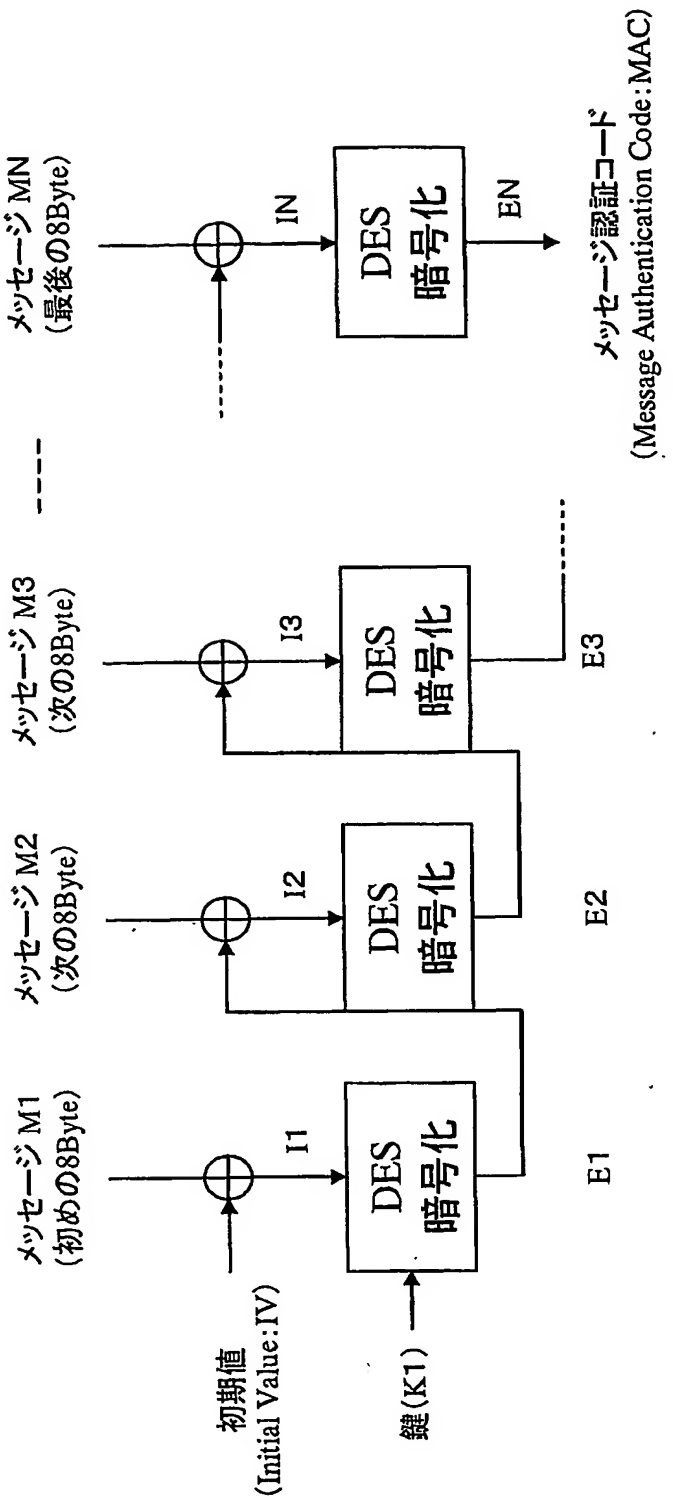

メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
EN
メッセージ認証コード
(Message Authentication Code:MAC)
:排他的論理和処理(8バイト単位)

FIG. 9

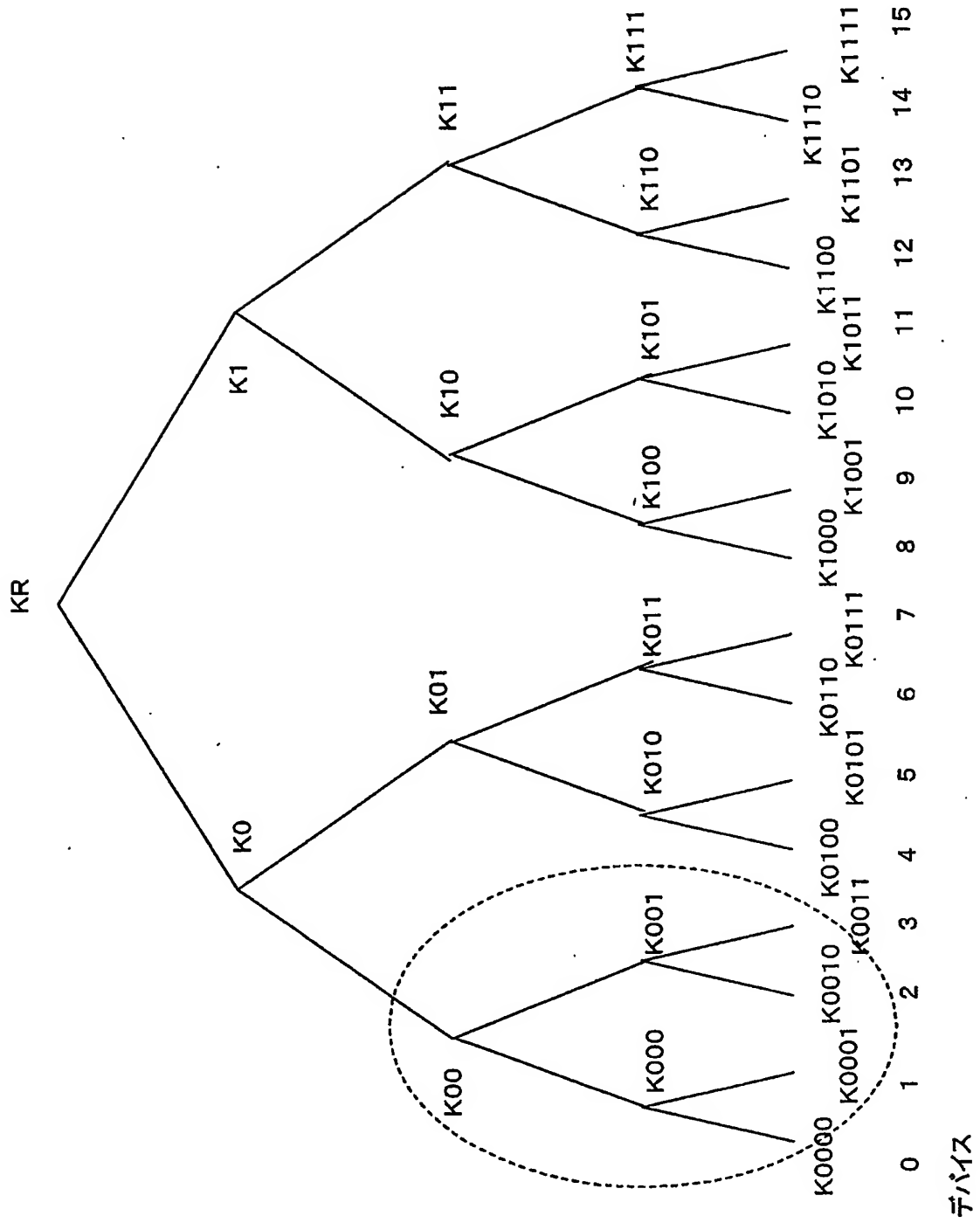

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

FIG. 10A

有効化キーブロック
(EKB:Enabling Key Block)例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 10B

有効化キーブロック
(EKB:Enabling Key Block)　例2

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 11

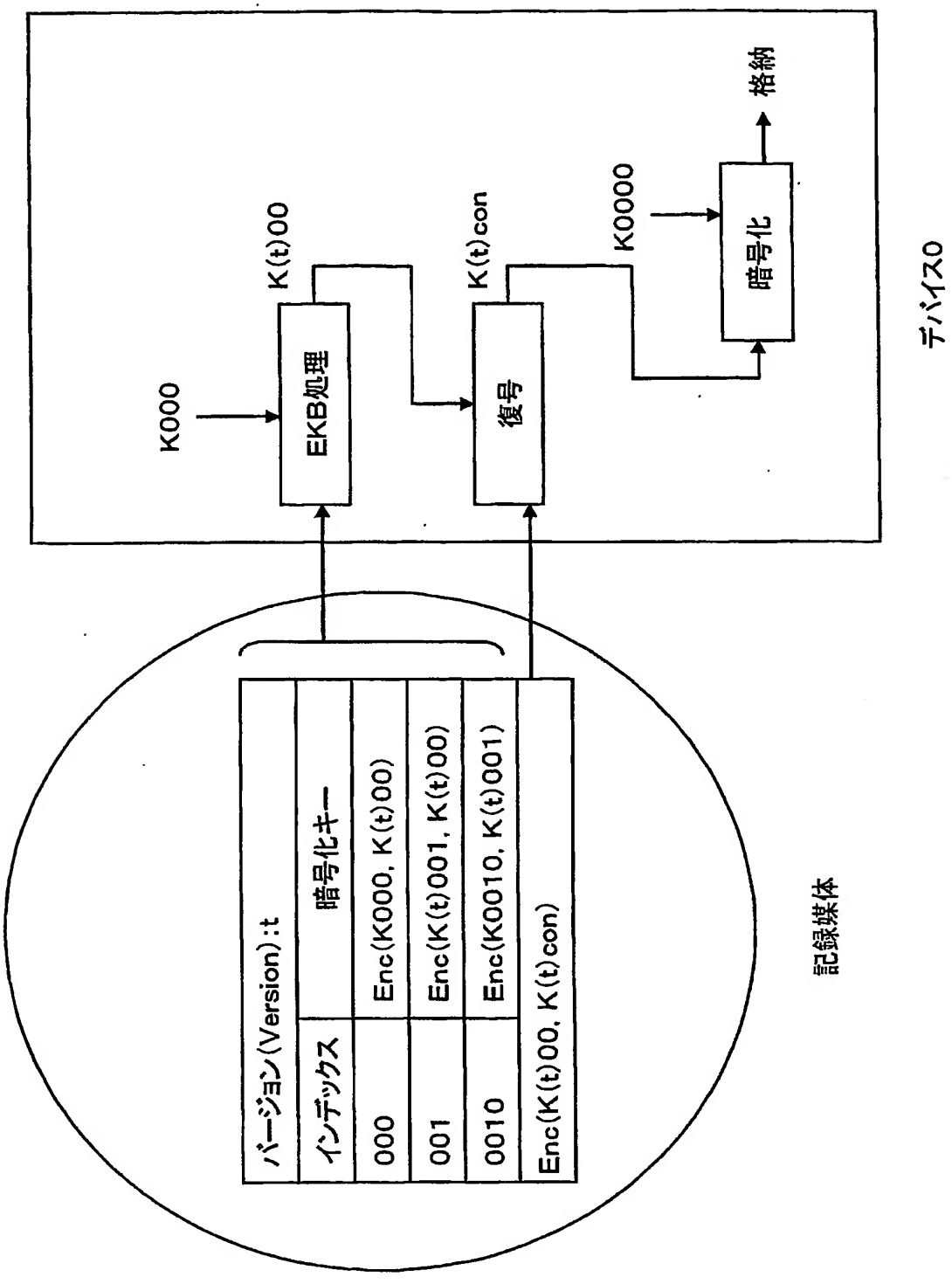

K000
EKB処理
K(t)00
復号
K(t)con
K0000
暗号化
格納
デバイス0
記録媒体
バージョン(Version):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)

FIG. 12

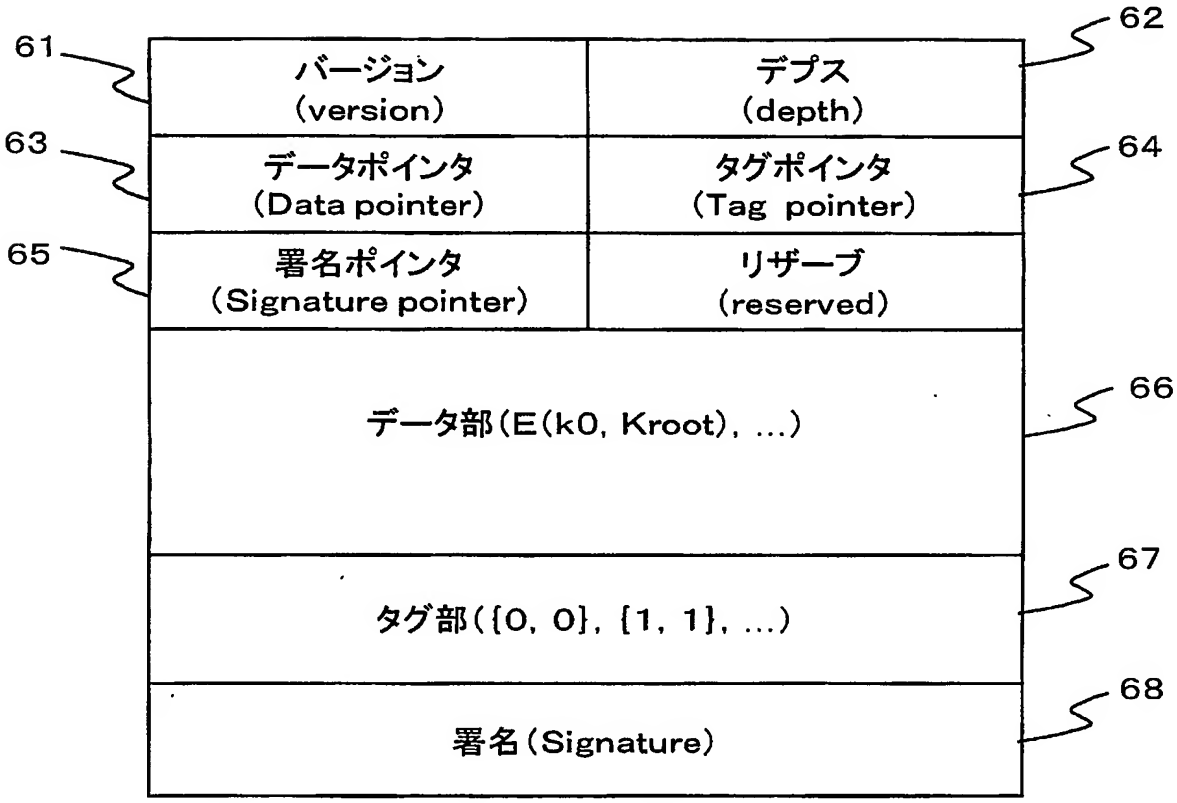

61
62
バージョン
(version)
デプス
(depth)
63
64
データポインタ
(Data pointer)
タグポインタ
(Tag pointer)
65
署名ポインタ
(Signature pointer)
リザーブ
(reserved)
66
データ部(E(k0, Kroot), ...)
67
タグ部({0, 0}, {1, 1}, ...)
68
署名(Signature)

FIG. 13A

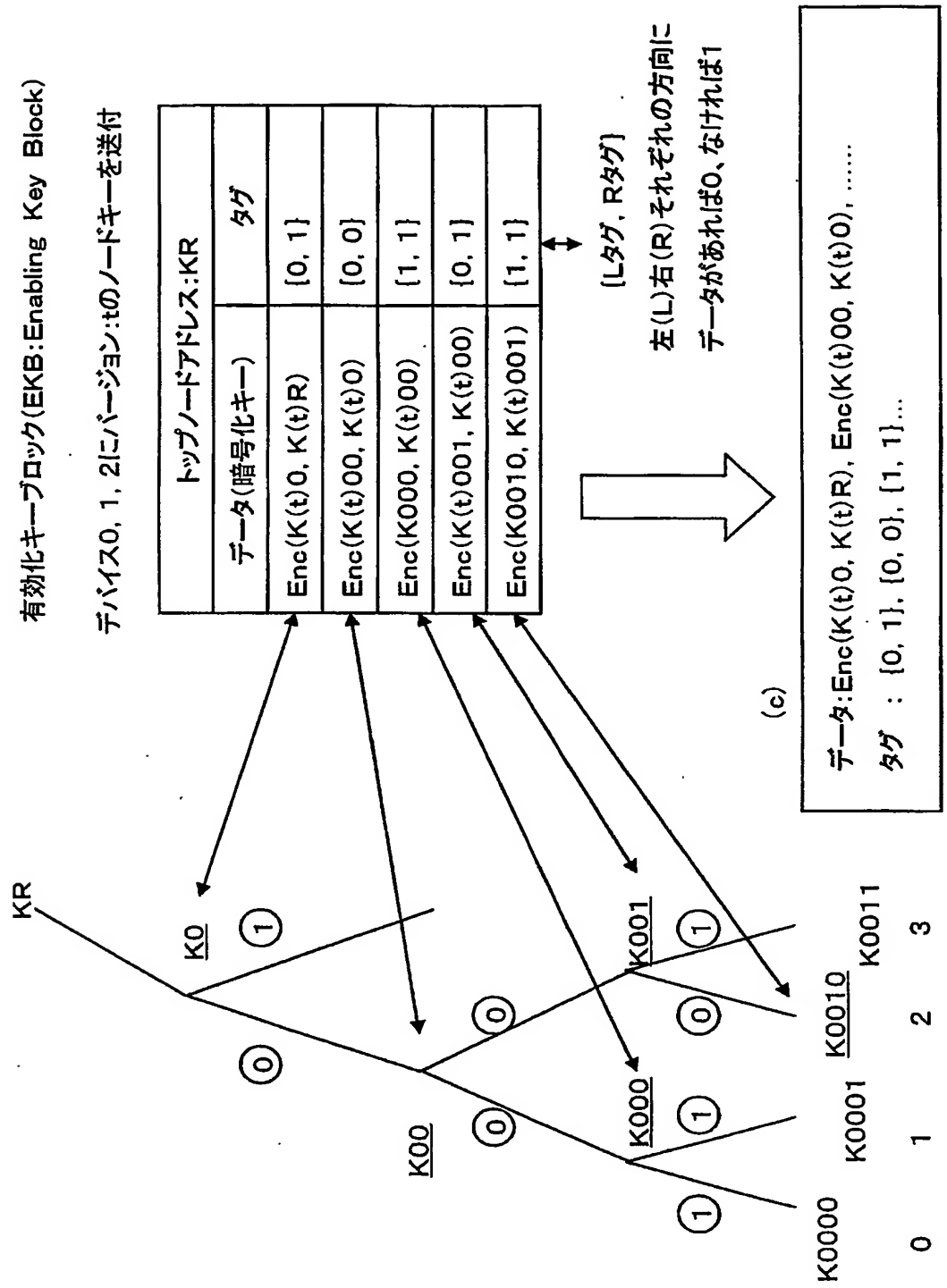


FIG. 13B

FIG. 14

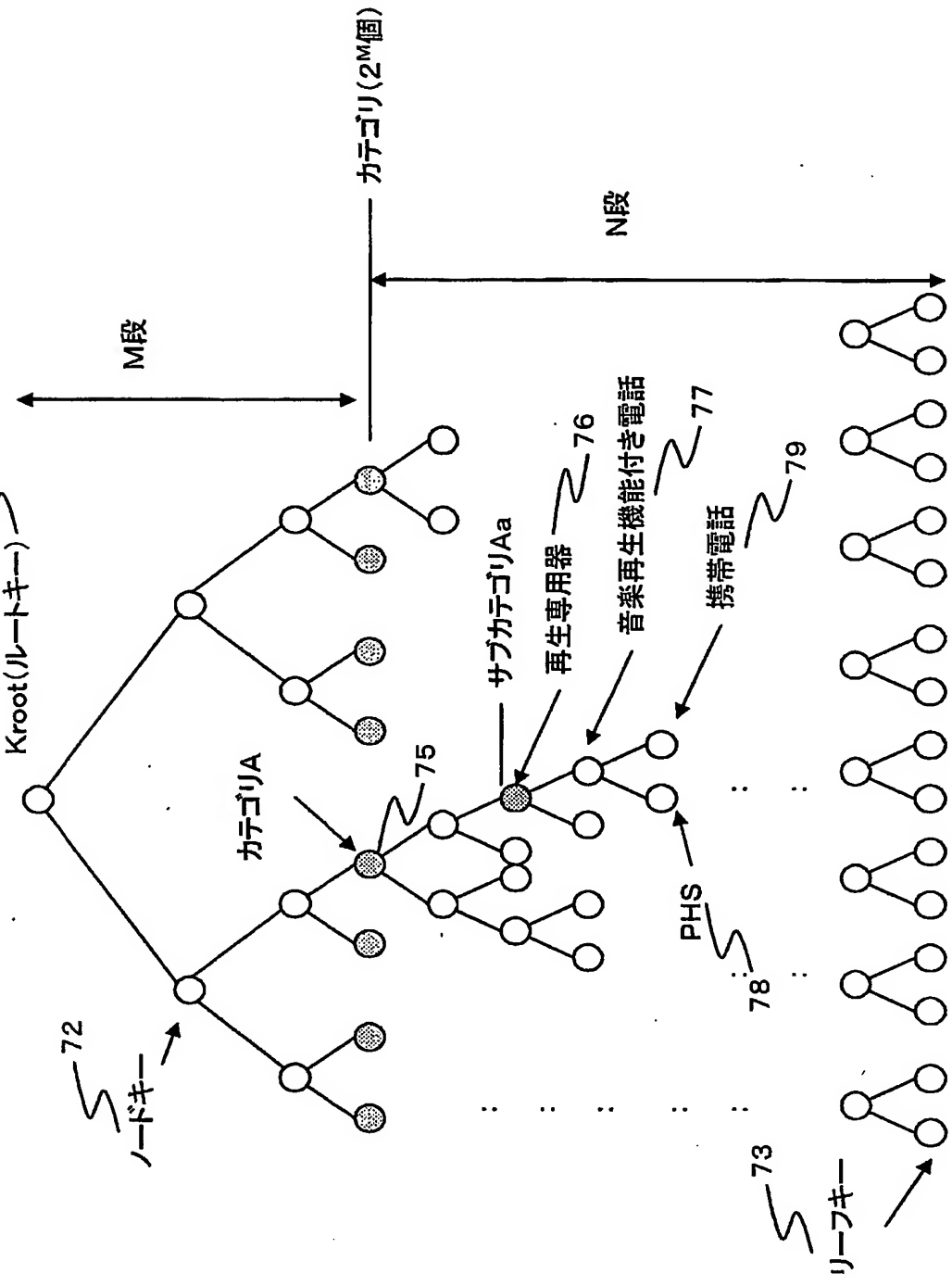

Kroot(ルートキー)
71
M段
カテゴリ(2^M個)
N段
カテゴリA
75
サブカテゴリAa
再生専用器
76
音楽再生機能付き電話
77
携帯電話
79
PHS
78
72
ノードキー
73
リーフキー

FIG. 15

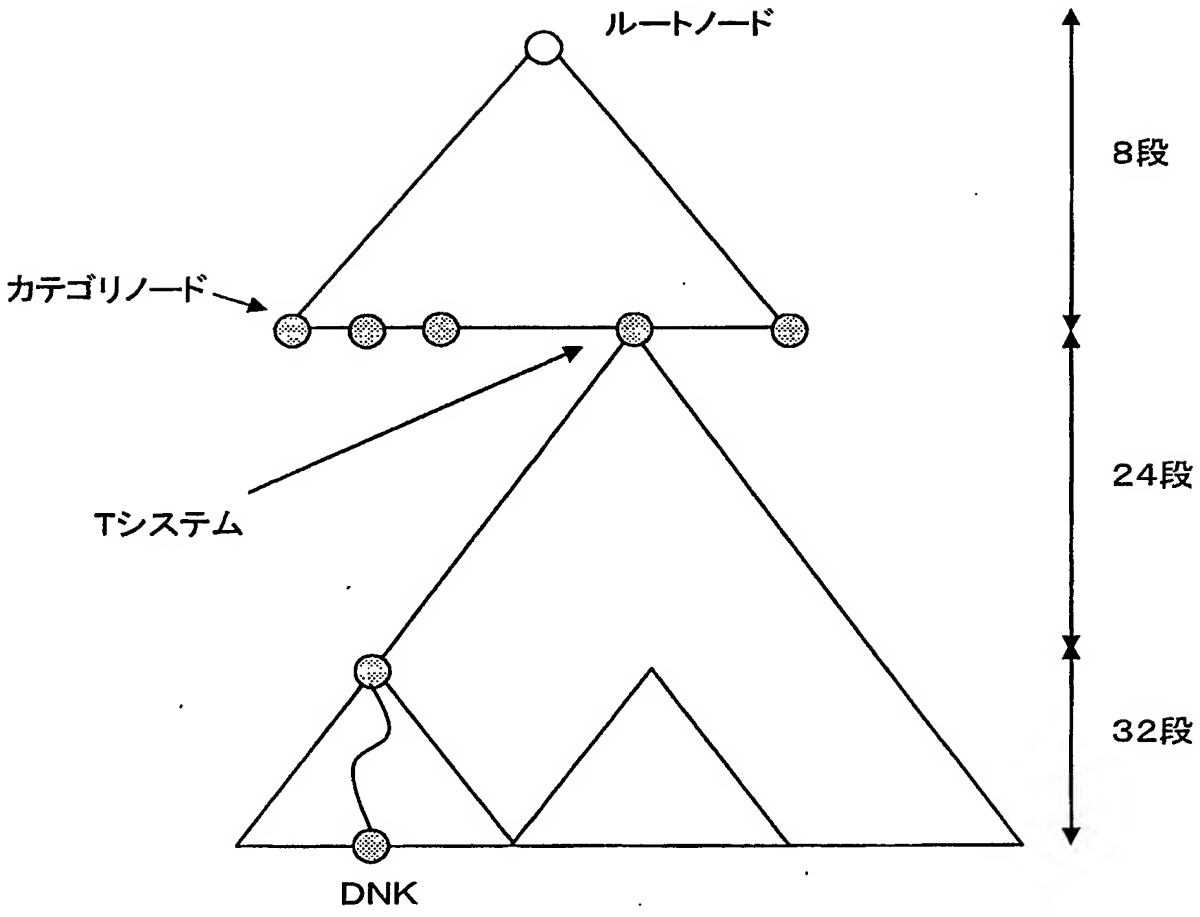


FIG. 16

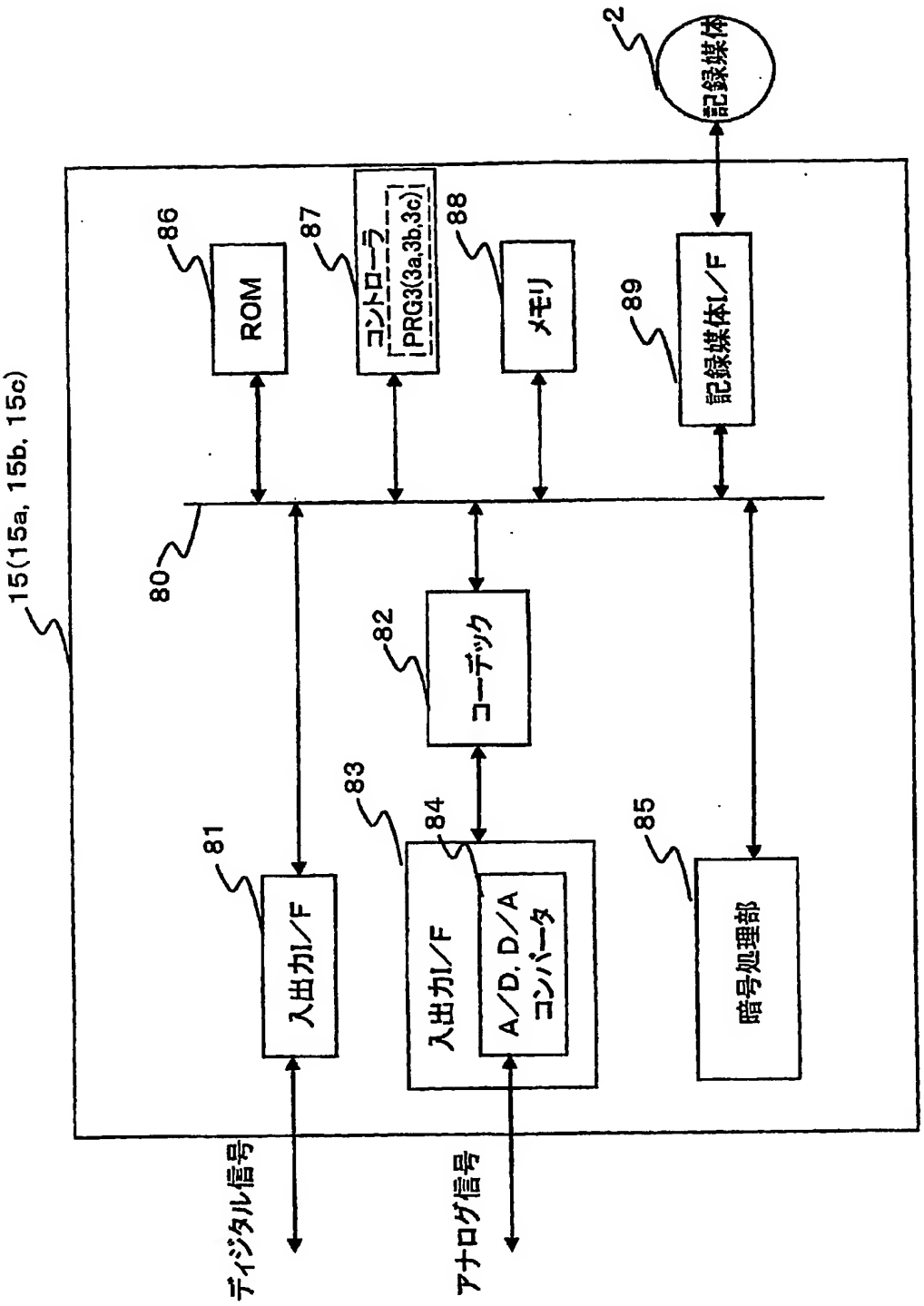

2
記録媒体
15(15a, 15b, 15c)
80
86
ROM
87
コントローラ
[PRG3(3a,3b,3c)]
88
メモリ
89
記録媒体I/F
82
コーデック
83
84
入出力I/F
A/D, D/A
コンバータ
81
入出力I/F
85
暗号処理部
ディジタル信号
アナログ信号

FIG. 17

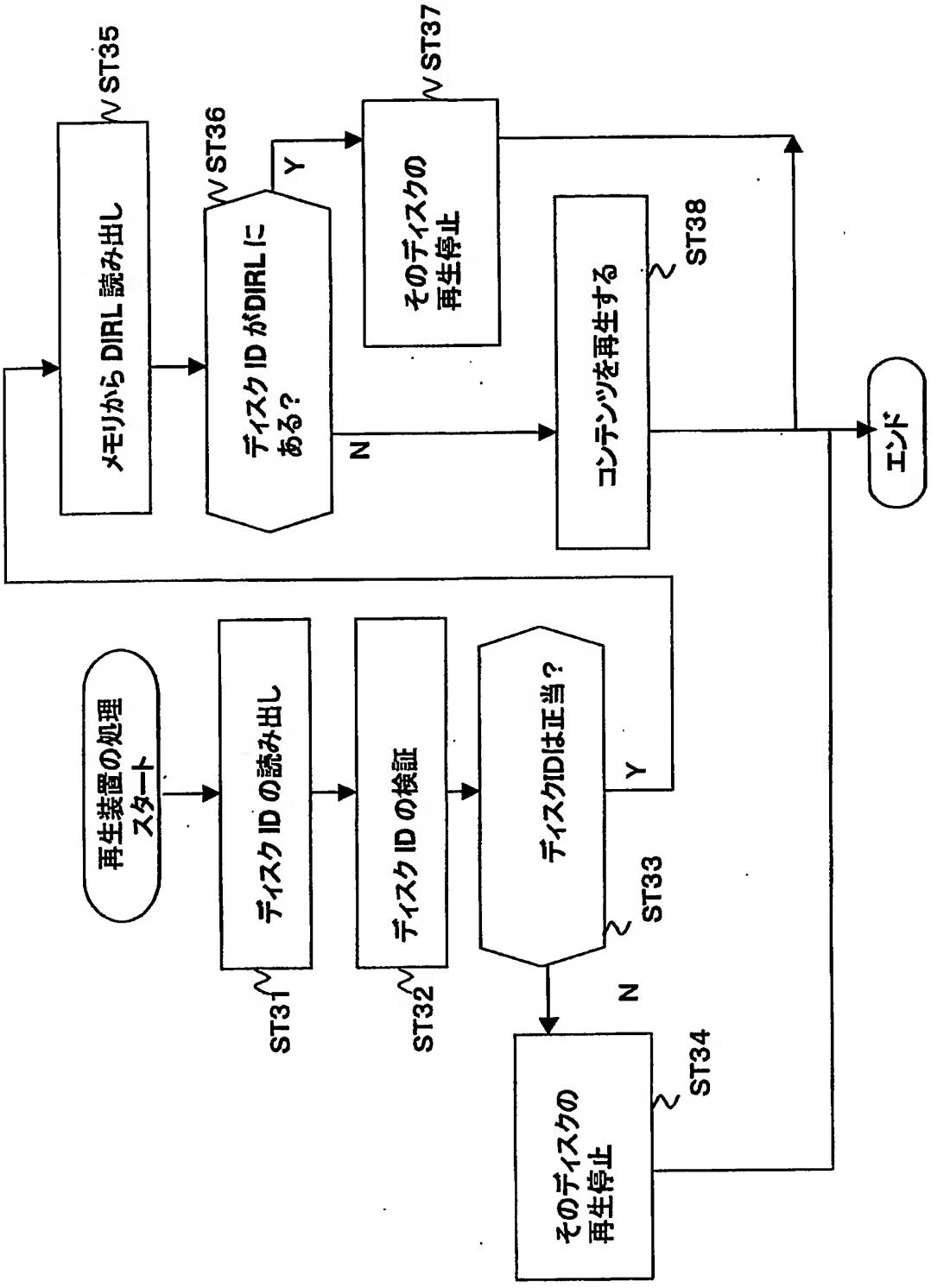

再生装置の処理スタート
ディスク ID の読み出し
ST31
ディスク ID の検証
ST32
ディスクIDは正当？
ST33
Y
N
そのディスクの再生停止
ST34
メモリから DIRL 読み出し
ST35
ディスク ID がDIRL にある？
ST36
Y
N
そのディスクの再生停止
ST37
コンテンツを再生する
ST38
エンド

FIG. 18

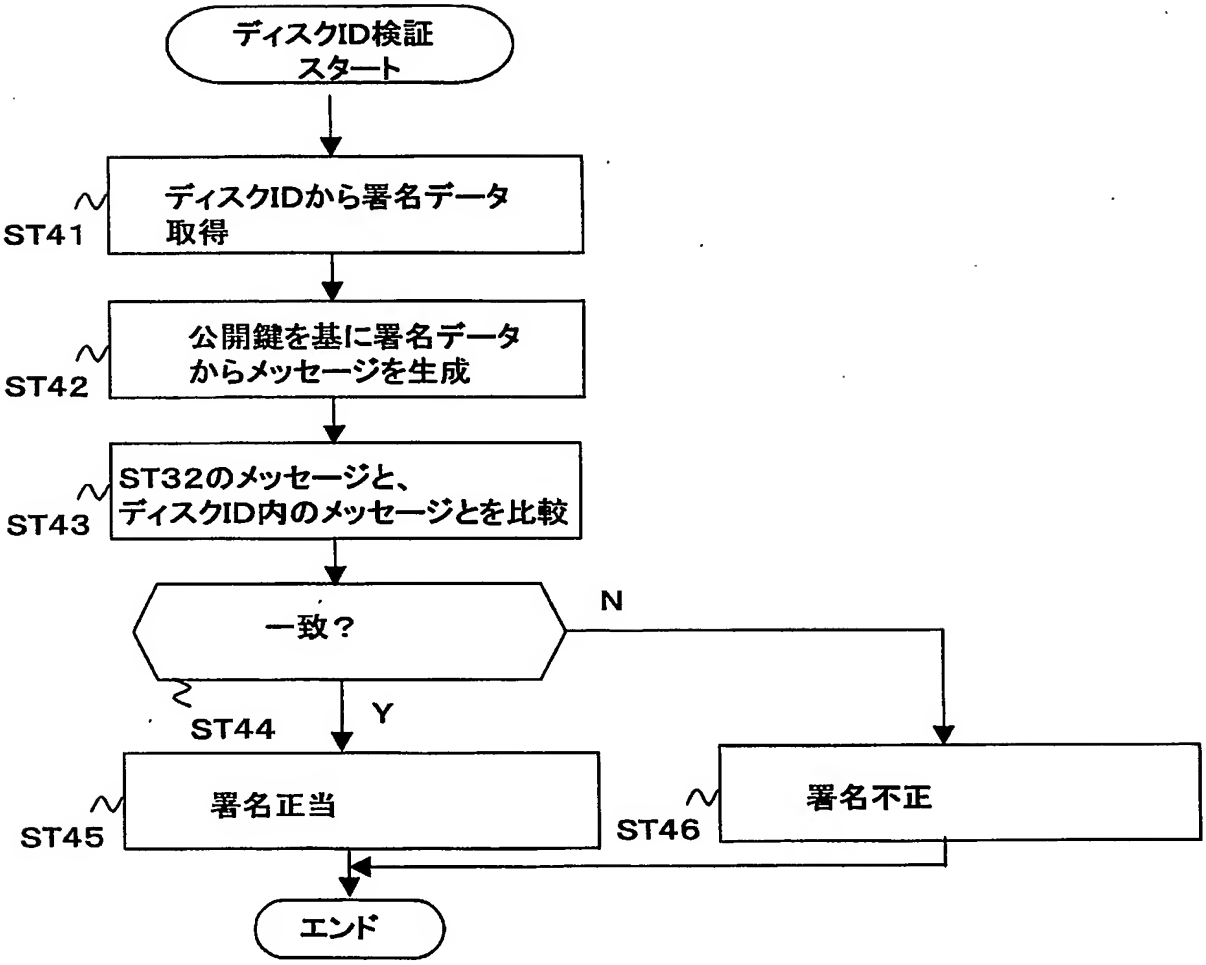

ディスクID検証
スタート
ST41
ディスクIDから署名データ
取得
ST42
公開鍵を基に署名データ
からメッセージを生成
ST43
ST32のメッセージと、
ディスクID内のメッセージとを比較
一致？
N
ST44
Y
ST45
署名正当
ST46
署名不正
エンド

FIG. 19

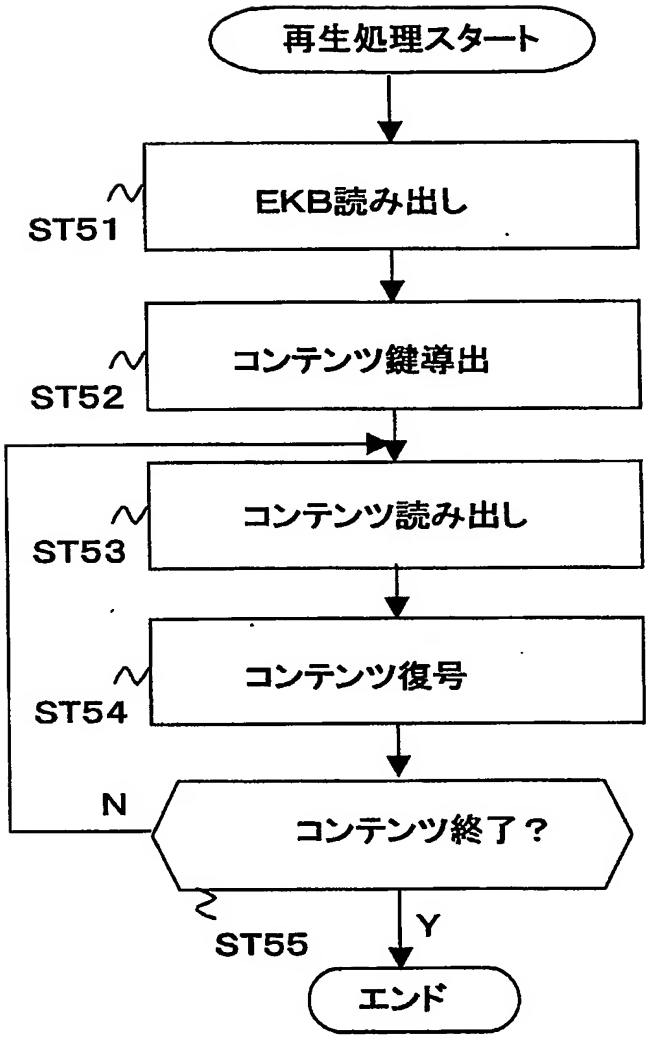

再生処理スタート
EKB読み出し
ST51
コンテンツ鍵導出
ST52
コンテンツ読み出し
ST53
コンテンツ復号
ST54
N
コンテンツ終了？
ST55
Y
エンド

FIG. 20

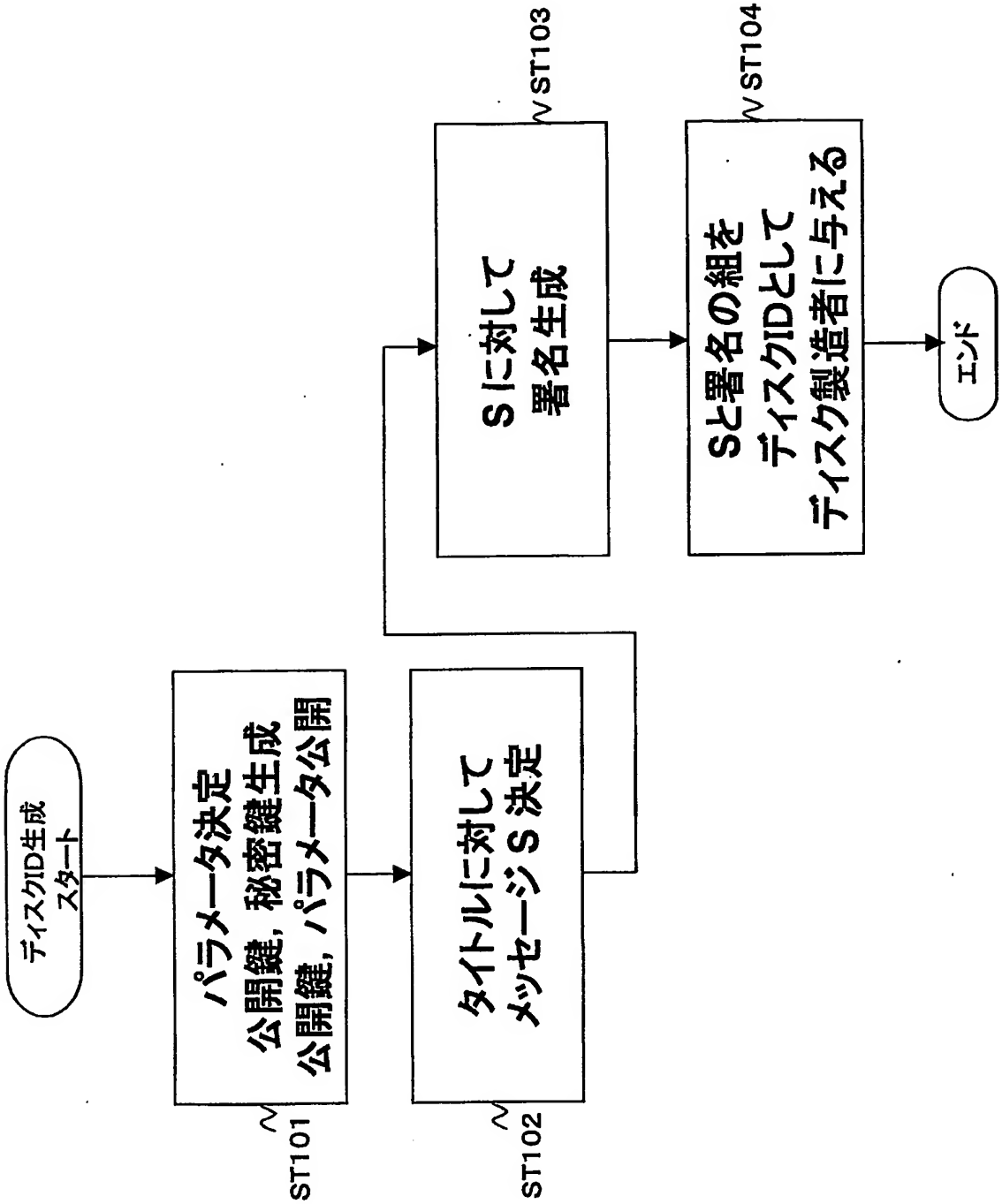

ディスクID生成
スタート
パラメータ決定
公開鍵，秘密鍵生成
公開鍵，パラメータ公開
ST101
タイトルに対して
メッセージS決定
ST102
Sに対して
署名生成
ST103
Sと署名の組を
ディスクIDとして
ディスク製造者に与える
ST104
エンド

FIG. 21

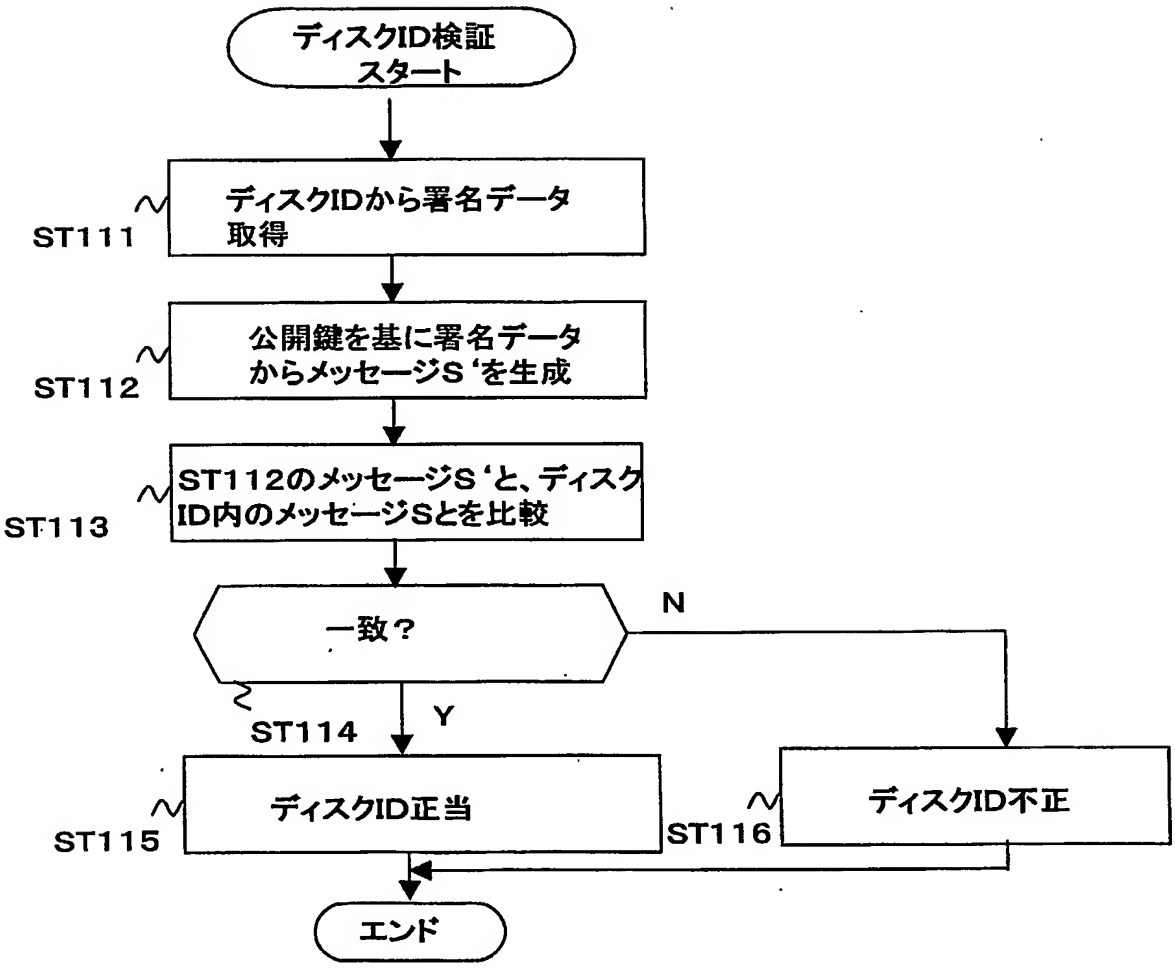

ディスクID検証
スタート
ST111
ディスクIDから署名データ
取得
ST112
公開鍵を基に署名データ
からメッセージS'を生成
ST113
ST112のメッセージS'と、ディスク
ID内のメッセージSとを比較
一致？
N
ST114
Y
ST115
ディスクID正当
ST116
ディスクID不正
エンド

FIG. 22

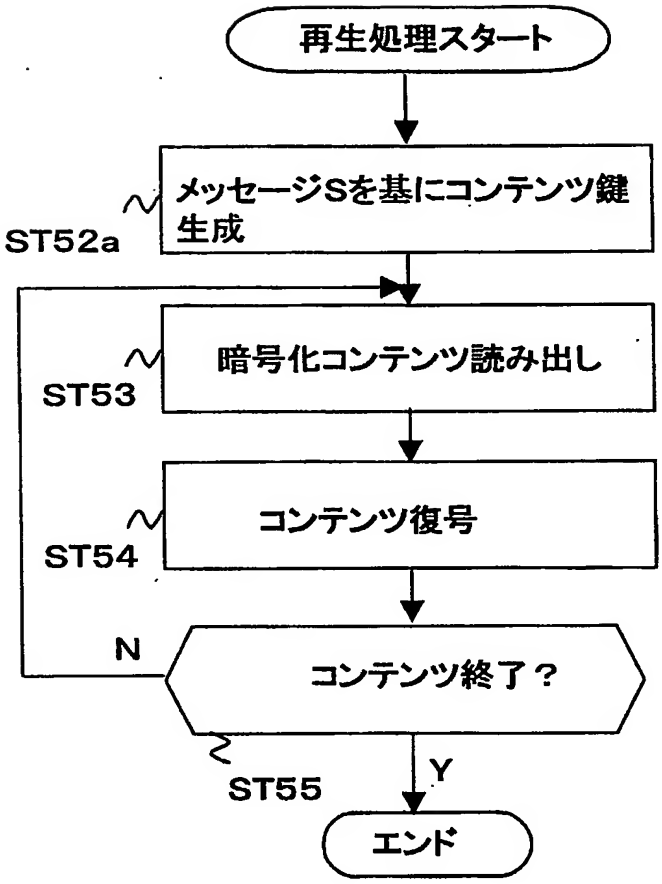

再生処理スタート
メッセージSを基にコンテンツ鍵生成
ST52a
暗号化コンテンツ読み出し
ST53
コンテンツ復号
ST54
コンテンツ終了？
N
ST55
Y
エンド

FIG. 23

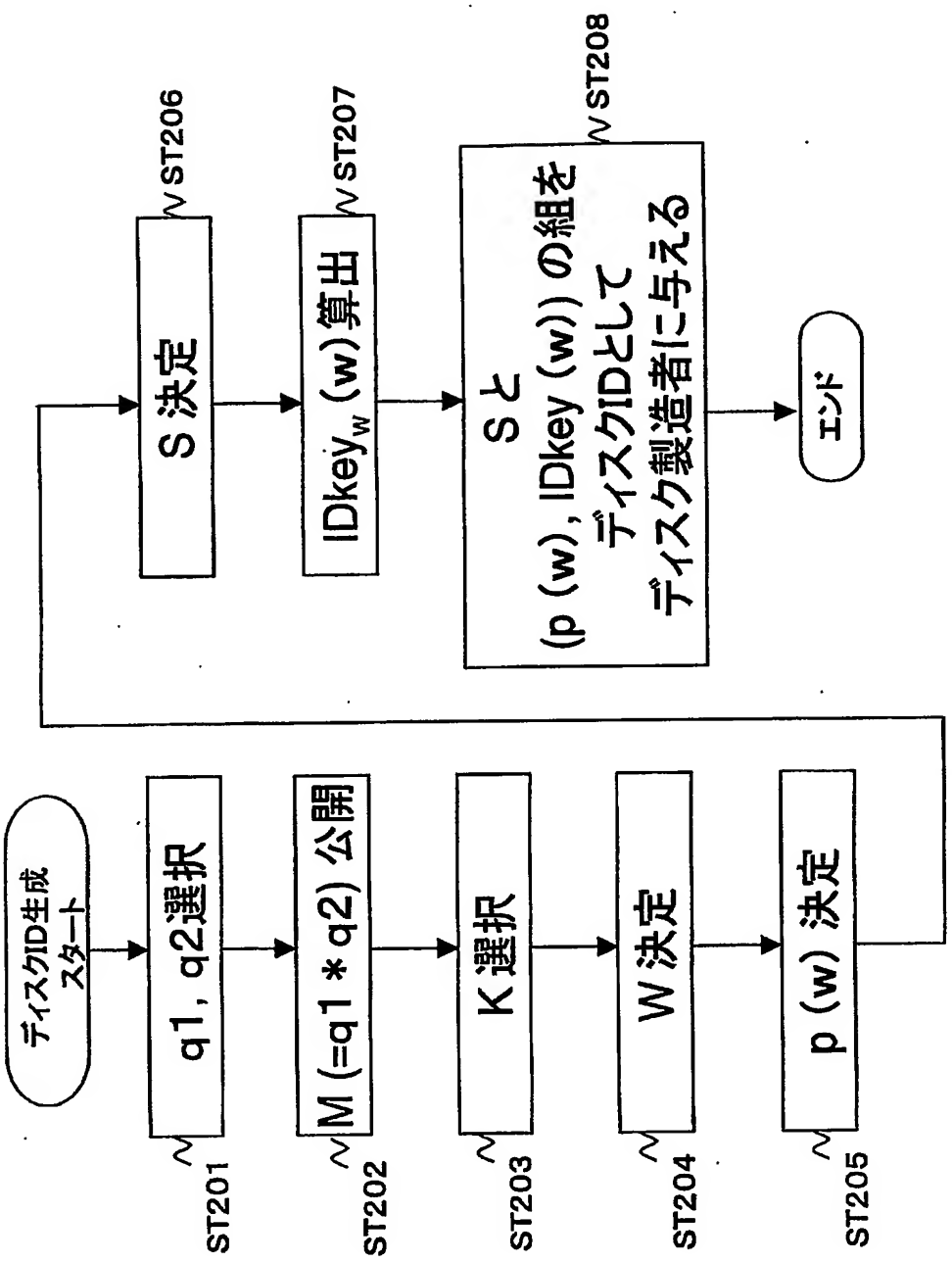

ディスクID生成
スタート
q1, q2選択
ST201
M (=q1 * q2) 公開
ST202
K 選択
ST203
W 決定
ST204
p (w) 決定
ST205
S 決定
ST206
IDkey$_w$ (w) 算出
ST207
S と
(p (w), IDkey (w)) の組を
ディスクIDとして
ディスク製造者に与える
ST208
エンド

FIG. 24

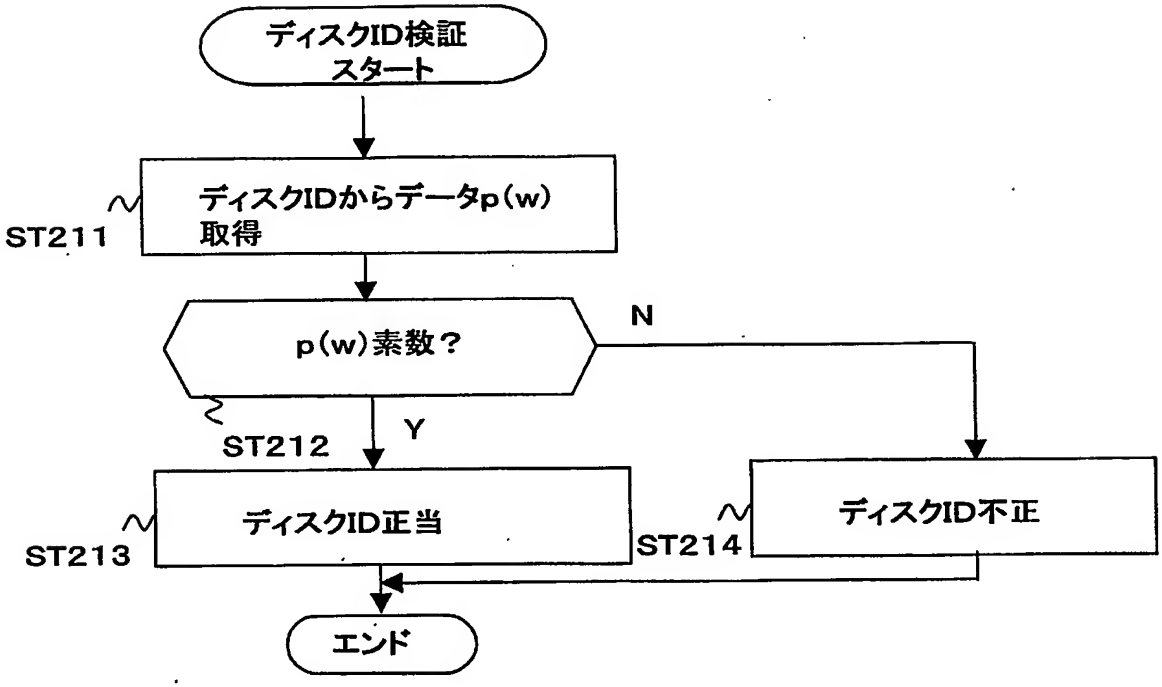

ディスクID検証
スタート
ST211
ディスクIDからデータp(w)
取得
p(w)素数？
N
Y
ST212
ディスクID正当
ST213
ディスクID不正
ST214
エンド

FIG. 25

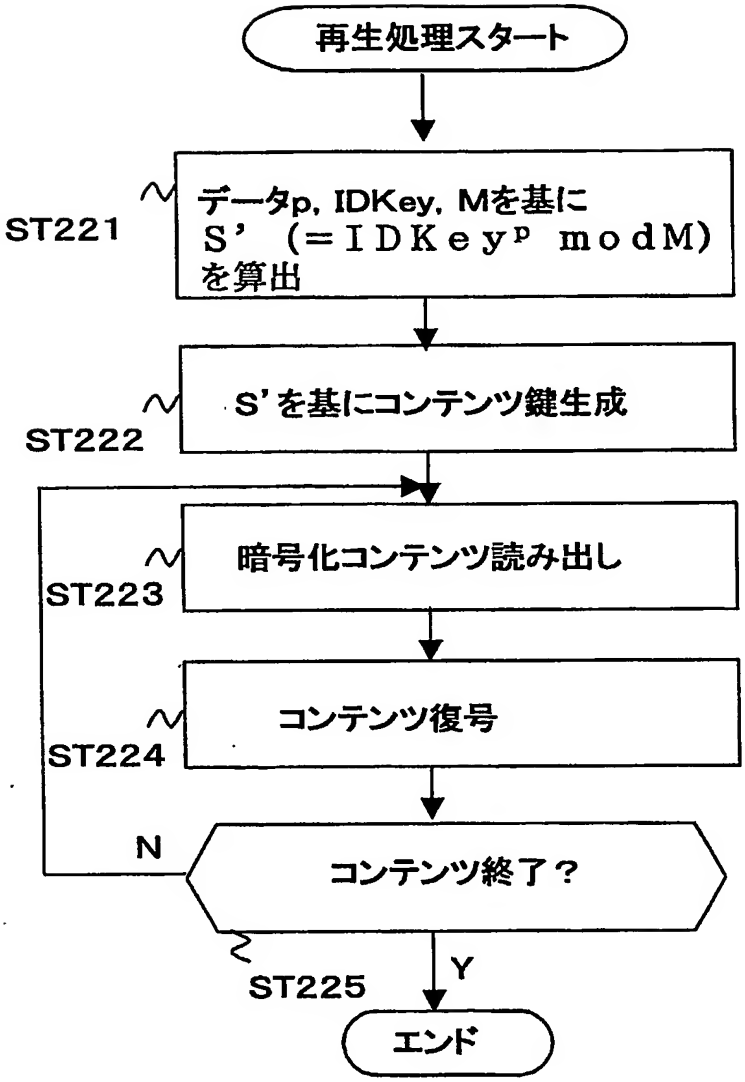

再生処理スタート
ST221
データp, IDKey, Mを基に
S' (=IDKey^p modM)
を算出
S'を基にコンテンツ鍵生成
ST222
暗号化コンテンツ読み出し
ST223
コンテンツ復号
ST224
N
コンテンツ終了？
ST225
Y
エンド

FIG. 26

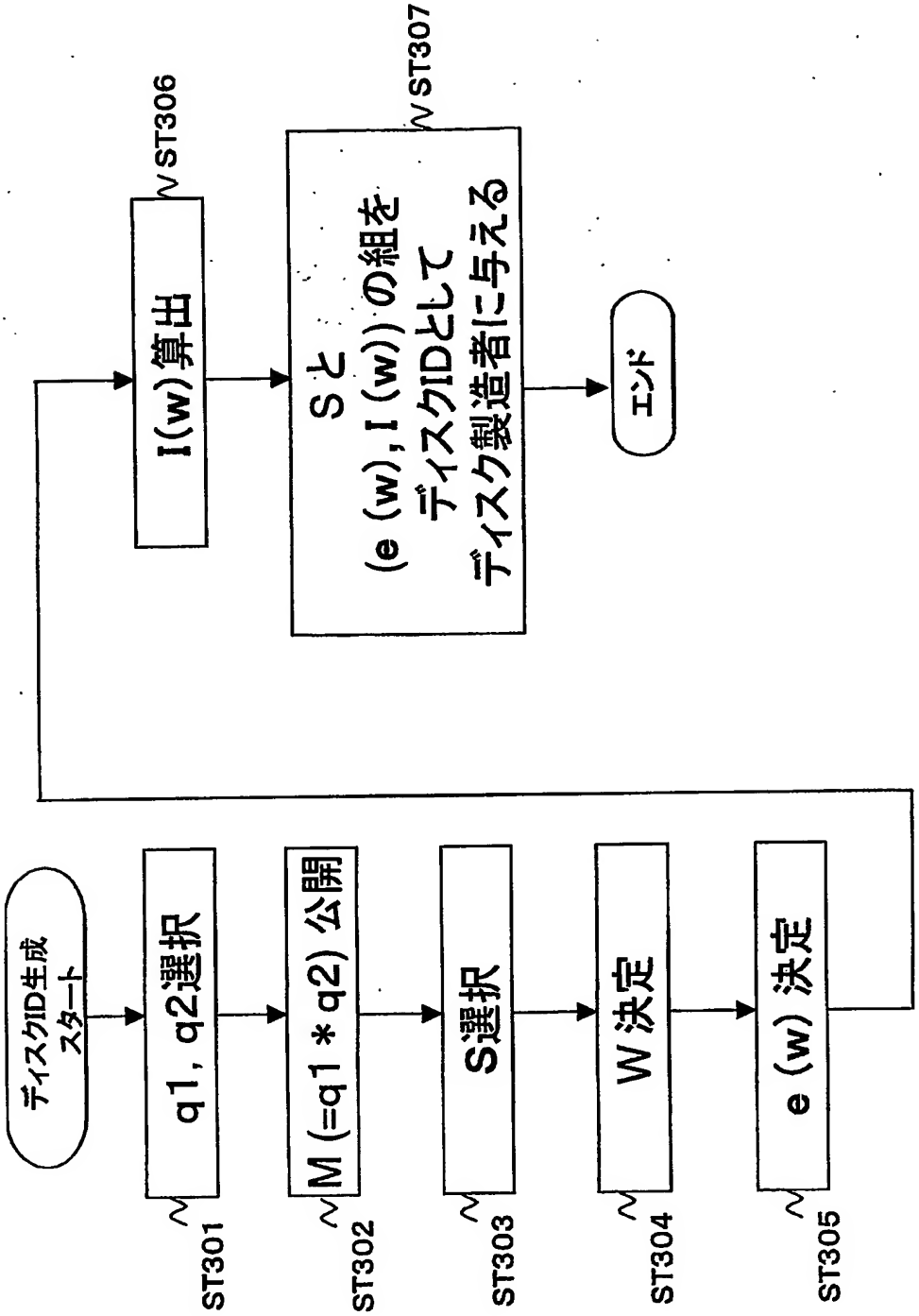
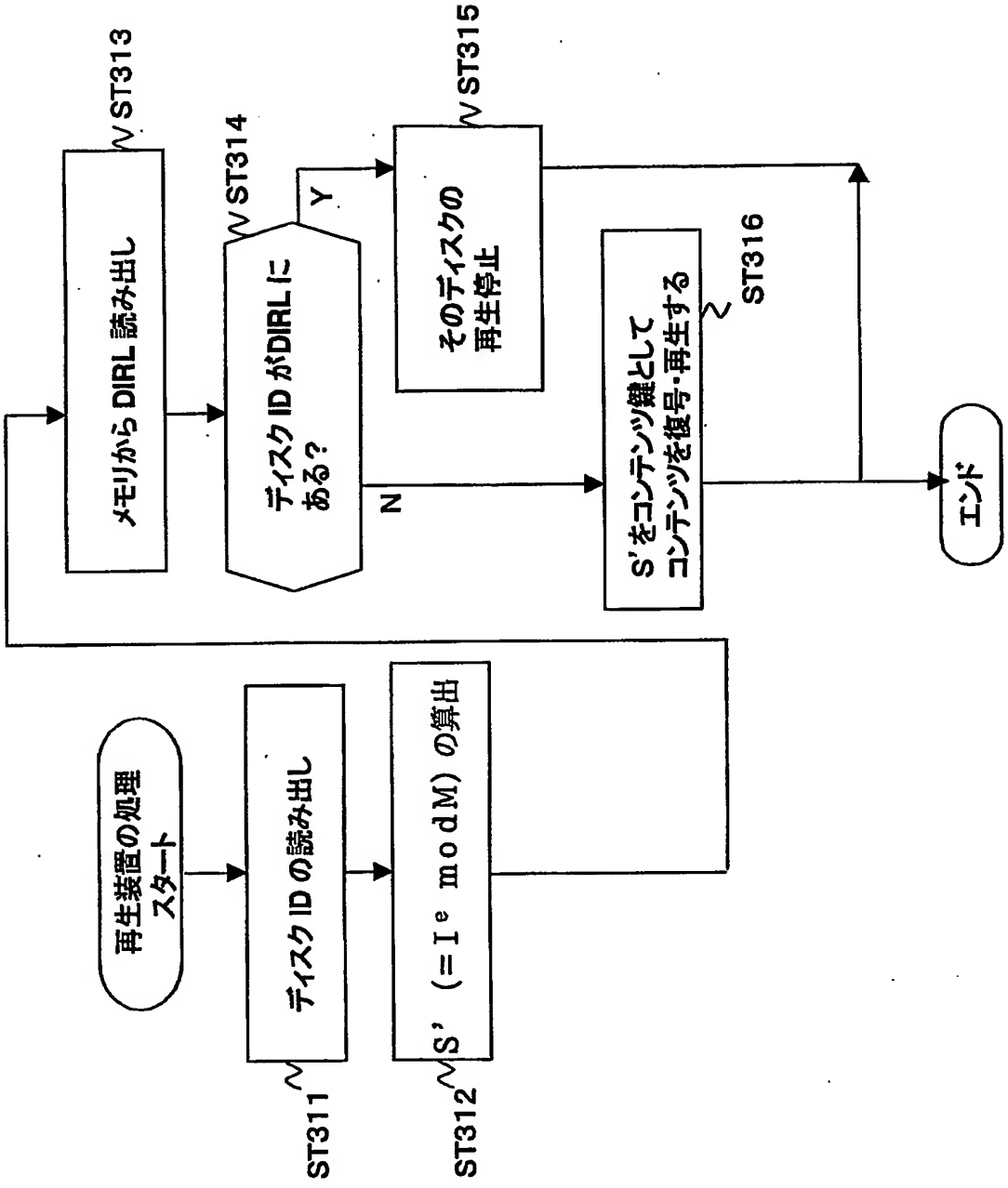

ディスクID生成
スタート
q1, q2選択
ST301
M (=q1 * q2) 公開
ST302
S選択
ST303
W 決定
ST304
e (w) 決定
ST305
I(w)算出
ST306
Sと
(e (w), I (w)) の組を
ディスクIDとして
ディスク製造者に与える
ST307
エンド

FIG. 27


再生装置の処理スタート
ディスクIDの読み出し
ST311
S'（=I^e mod M）の算出
ST312
メモリからDIRL読み出し
ST313
ディスクIDがDIRLにある？
ST314
Y
N
そのディスクの再生停止
ST315
S'をコンテンツ鍵としてコンテンツを復号・再生する
ST316
エンド

符　号　の　説　明

２，２ａ，２ｂ，２ｃ…ディスク型記録媒体

１２，１２ａ，１２ｂ，１２ｃ…管理装置

１３…コンテンツ提供装置

１４…ディスク製造装置

１５，１５ａ，１５ｂ，１５ｃ…再生装置

２１…バス

２２…メインメモリ

２３…セキュアメモリ

２４…入出力インタフェース

２５…記録媒体インタフェース

２６…演算ユニット

２７…コントローラ

８０…バス

８１…入出力インタフェース

８２…コーデック

８３…入出力インタフェース

８４…コンバータ

８５…暗号処理部

８６…ＲＯＭ

８７…コントローラ

８８…メモリ

８９…記録媒体インタフェース

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/006324

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B20/10, G11B20/12, G11B27/00, G06F12/14, H04L9/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B20/10, G11B20/12, G11B27/00, G06F12/14, H04L9/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-132457 A (Victor Company Of Japan, Ltd.), 10 May, 2002 (10.05.02), Full text; Figs. 1 to 11 (Family: none)	1-4,9-12, 16-19,23-26
X	JP 11-212454 A (NHK Spring Co., Ltd.), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 10 (Family: none)	1-4,9-12, 6-19,23-26
X	JP 11-202766 A (Canon Inc.), 30 July, 1999 (30.07.99), Full text; Figs. 1 to 5 & US 6298153 B1	1-4,9-12, 16-19,23-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
02 September, 2004 (02.09.04)

Date of mailing of the international search report
21 September, 2004 (21.09.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/006324

Box No. II **Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III **Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

This application does not satisfy the requirement of unity of invention because of the reason given on the extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-4, 9-12, 16-19, 23-26

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

The inventions of claims 1-4, 9-12, 16-19, 23-26 have "a special technical feature" relating to "assigning a plurality of signature data to a plurality of different recording media."

The inventions of claims 5-8, 13-15, 20-22, 27-31 have "a special technical feature" relating to "authentication of validity of the identification data assigned to the recording medium."

The inventions of claims 32-33 have "a special technical feature" relating to "a recording medium for recording encrypted data and recording identification data identifying the recording medium containing the content key data."

Recording predetermined identification data on a recording medium so as to prevent unauthorized copying is a known configuration. And the public key encryption method using a secret key and a public key is a known technique.

Accordingly, these inventions have only the known configurations and are not so linked as to have a special technical feature.

There is no technical relationship among those inventions involving one or more of the same or corresponding technical features. Consequently, the inventions are not so linked as to form a single general inventive concept.

国際調査報告

国際出願番号　PCT／JP2004／006324

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G11B 20／10 G11B 20／12 G11B 27／00
G06F 12／14 H04L 9／00 H04L 9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G11B 20／10 G11B 20／12 G11B 27／00
G06F 12／14 H04L 9／00 H04L 9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP　2002-132457　A（日本ビクター株式会社） 2002. 05. 10　，全文，　第1－11図（ファミリーなし）	1-4, 9-12, 16-19, 23-26
X	JP　11-212454　A（日本発条株式会社） 1999. 08. 06　，全文，　第1－10図（ファミリーなし）	1-4, 9-12, 16-19, 23-26

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 02. 09. 2004	国際調査報告の発送日 21. 9. 2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 前田　祐希　5Q　2946 電話番号　03－3581－1101　内線　3590

様式PCT／ISA／210（第2ページ）（2004年1月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ　11-202766　Ａ（キャノン株式会社） 1999．07．30　，全文，　第1－5図 ＆　ＵＳ　6298153　Ｂ1	1-4, 9-12, 16-19, 23-26

国際調査報告　　国際出願番号　ＰＣＴ／ＪＰ２００４／００６３２４

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

単一性を満たさない理由は、特別ページに記載した。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☒ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

請求の範囲　１－４，　９－１２，　１６－１９，　２３－２６

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

請求の範囲１－４、９－１２、１６－１９、２３－２６の「特別な技術的特徴」は、「複数の署名データを識別データとして異なる複数の記録媒体にそれぞれ割当てる」ことに関するものである。

請求の範囲の５－８、１３－１５、２０－２２、２７－３１の「特別な技術的特徴」は、「記録媒体に割当てられた識別データの正当性を検証する」ことに関するものである。

請求の範囲の３２－３３の「特別な技術的特徴」は「暗号データを記録する記録媒体であって、コンテンツ鍵データを含む記録媒体を識別する識別データを記録するする」ことに関するものである。

不正コピーを防止するために、記録媒体に所定の識別データを記録することは、周知の構成である。そして、秘密鍵、公開鍵を用いる公開鍵暗号化方式は、周知技術である。
よって、これらの発明は、上記の周知の構成のみでそれぞれの発明が特別な技術的特徴を含む関係があるとは認められない。

よって、これらの発明は、一又は二以上の同一又は対応する特別な技術的特徴を含む技術的な関係にないから、単一の一般的発明概念を形成するように連関しているものとは認められない。